LEGISLATION

General Data Protection Regulation

There are 6 General Data Protection Regulation principles which the Trust must adhere to. Data must be:

1 Fairly and lawfully processed
2 Used only for specified and lawful purposes
3 Adequate, relevant and not excessive
4 Kept accurately and up to date
5 Not kept for longer than necessary
6 Kept securely and protected against accidental disclosure, loss or damage

Common Law Duty of Confidence

"Information given or received in confidence, obtained for one purpose, must not be disclosed or used for another purpose without the consent of the provider of the information"

Article 8— HUMAN RIGHTS ACT 1998

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.

The Care Record Guarantee

The Care Record Guarantee sets out the rules that govern how patient information is used in the NHS and the control the patient can have over this. It looks at an individuals rights of access to their own information, how information will be shared and how decisions on sharing information will be made. Everyone who works for the NHS must comply with this guidance.

FOR FURTHER ADVICE OR INFORMATION CONTACT:

Information Governance

sfh-tr.information.governance@nhs.net

Caldicott Guardian

Head of Corporate Affairs & Company Secretary

Senior Information Risk Owner (SIRO)

Chief Finance Officer

USEFUL WEBSITES

Information Commissioner's Officer

NHS Digital

Department of Health

Care Record Guarantee

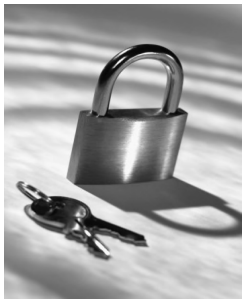
Sherwood Forest Hospitals NHS Foundation Trust
King's Mill Hospital
Mansfield Road
Sutton in Ashfield
Nottinghamshire
NG17 4JL
Tel: 01623 622515

Sherwood Forest Hospitals NHS Foundation Trust Website

NHS
Sherwood Forest Hospitals
NHS Foundation Trust

Dedicated to Outstanding care

CONFIDENTIALITY CODE OF CONDUCT



Security and Confidentiality of Personal Confidential Information

INTRODUCTION

All employees of the Trust are responsible for maintaining confidentiality of staff and patients, and this duty of confidentiality is written into employment contracts.

Staff are authorised to have access to personal confidential data on a need to know basis in order for them to perform their duties. Accessing data that is not needed to carry out work or passing data to someone who is not authorised to receive it is a breach of confidentiality which could result in disciplinary action.

Serious breaches of the General Data Protection Regulation may result in monetary penalties from the Information Commissioners Office (ICO).

The Caldicott Principles

The Information Governance Review March 2013 built on the previous Caldicott Report to look at the balance between safeguarding patients' sensitive information and encouraging responsible information sharing.

It resulted in a few amendments to the principles and the addition of a further principle:

1. Justify the purpose for using personal confidential data
2. Do not use personal confidential data unless it is absolutely necessary
3. Use the minimum necessary personal confidential data
4. Access to personal confidential data should be on a strict need-to-know basis
5. Everyone with access to personal confidential data must be aware of their responsibilities
6. Every use of personal confidential data must be lawful
7. The duty to share information can be as important as the duty to protect patient confidentiality.

The term 'personal confidential data' refers to any information held about an individual who can be identified from that information. For example, name, address, postcode, NHS number, etc. Any personal confidential data, non-clinical or clinical, must be treated as confidential.

BASIC PRINCIPLES

Any personal confidential data given for one purpose must not be used for another purpose without the consent of the individual concerned.

An individual's right to confidentiality is protected by ethics and law. Individuals using Trust services or employed by the Trust, have a legal right to know what data is being collected and why, as well as the purposes for sharing that data.

An individual has the right to choose whether or not to disclose their personal data and can change their decision at any point.

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 individual requesting data. This ensures data is only passed on to those who have a right to see it. All staff should understand their responsibility to protect the confidential data they collect and follow the rules and guidance available to them.

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

Consent

To be valid, consent must be given voluntarily and freely. A patient/employee must be fully informed and know what the proposed use or disclosures of their personal data will be.

Explicit consent must always be sought from a patient in order to use their personal data in ways that do not directly contribute to their healthcare.

It may be lawful in certain circumstances to share personal data without consent (such as investigating serious crime, safeguarding children, or justified in the public interest).

INFORMATION SECURITY

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

- Do not use someone else's password to gain access to information held on computers
- No personal confidential data should be held on any mobile devices (e.g. laptops, PDA's, memory sticks) unless it is encrypted to the approved standard.
- Faxing is not secure. Personal confidential data should be faxed only when there is no alternative and immediate receipt is necessary for clinical purposes. "Safe Haven"* procedures should be followed.
- Envelopes containing personal confidential data must be securely sealed, labelled 'confidential' and clearly addressed to a known contact
- Telephone validation procedures must be followed to confirm the identity of callers before information is given to them
- Staff must always ensure that Trust policy is followed when sending personal confidential data by email
- Follow the Trust's policies and procedures relating to Data Protection, confidentiality, information security and seek advice when in doubt.

If you are unsure whether to disclose information, consult your line manager and/or if necessary obtain advice from your organisation's Caldicott Guardian or Information Governance Lead.

* A Safe Haven is an agreed set of administrative and physical security procedures for minimising the risk of breach of confidentiality