



**QUICK REFERENCE TO  
CALDICOTT &  
THE DATA PROTECTION ACT 1998  
PRINCIPLES**



*Surrey Health Community*

# What is Caldicott?

The term Caldicott refers to a review commissioned by the Chief Medical Officer. A review committee, under the chairmanship of Dame Fiona Caldicott, investigated ways in which patient information is used in the NHS.

The review committee also made a number of recommendations aimed at improving the way the NHS handles and protects patient information.

These are summarised by:

**Six Information Management Principles.**

# The Six Caldicott Principles

- 1 Justify the purpose(s) of using confidential information**

---
- 2 Only use it when absolutely necessary**

---
- 3 Use the minimum that is required**

---
- 4 Access should be on a strict need-to-know basis**

---
- 5 Everyone must understand his or her responsibilities**

---
- 6 Understand and comply with the law**

# What is the Data Protection Act 1998?

**The Data Protection Act 1998 became law in March 2000. It sets standards which must be satisfied when obtaining, recording, holding, using or disposing of personal data.**

**These are summarised by 8 Data Protection Principles.**

As well as information held on computers, the Data Protection Act 1998 also covers most manual records e.g.

- Health
- Personnel
- Occupational Health
- Volunteers
- Finance
- Suppliers
- Contractors
- Card Indices

# The Data Protection Principles

**Personal data must be:**

- 1 Processed fairly and lawfully**
- 2 Processed for specified purposes**
- 3 Adequate, relevant and not excessive**
- 4 Accurate and kept up-to-date**
- 5 Not kept for longer than necessary**
- 6 Processed in accordance with the rights of data subjects**
- 7 Protected by appropriate security  
*(practical and organisational)***
- 8 Not transferred outside the EEA without adequate protection**

# Principle 1

## Processed fairly and lawfully

There should be no surprises, so... inform data subjects why you are collecting their information, what you are going to do with it and who you may share it with...

e.g. when formulating a research project remember to be open and transparent about what you will be doing with the information.

e.g. when working in a team, ensure that the patient/client is aware of who the members of the team are, and that all those involved with their care may need to see their notes.

● **Be open, honest and clear**



# Principle 2

## Processed only for specified purposes

Only use personal information for the purpose(s) for which it was obtained.

e.g. personal information on a Patient Administration System must only be used for healthcare purposes - not for looking up friends' addresses or birthdays.

- **Only share information outside your practice, team, home, ward, department or service if you are certain it is appropriate and necessary to do so.**
- **If in doubt, check first!**



# Principle 3

## Adequate, relevant and not excessive

Only collect and keep the information you require.

It is not acceptable to hold information unless you have a view as to how it will be used

Do not collect information “just in case it might be useful one day!”

e.g. taking both daytime and evening telephone numbers if you know you will only call in the day.

- **Explain all abbreviations**
- **Use clear legible writing**
- **Stick to the facts - avoid personal opinions and comments**



# Principle 4

## Accurate and kept up-to-date

Take care inputting information to ensure accuracy

How do you know the information is up-to-date?

What mechanisms do you have for checking the information is accurate and up-to-date?

e.g. each time a patient attends a clinic, they should be asked to confirm that their details are correct - address, telephone number etc.

- **Check existing records thoroughly before creating new records**
- **Avoid creating duplicate records**



# Principle 5

## Not kept for longer than necessary

- Follow retention guidelines

The Records Management: NHS Code of Practice

- Check your organisation's retention policy
- Ensure regular housekeeping/spring cleaning of your information
- Do not keep "just in case it might be useful one day!"
- Check your organisation's disposal policy
- Dispose of your information correctly



# Principle 6

## Processed in accordance with the rights of data subjects

- Subject access
- Prevention of processing
- Prevent processing for direct marketing
  - an end to junk mail and faxes!
- Automated decision taking
- Compensation
- Rectification/blocking/erasure
- Request an assessment



# Principle 7 (Practical)

## Protected by appropriate security

- Ensure security of confidential faxes by using Safe Haven/Secure faxes
- **ALWAYS** keep confidential papers locked away
- Do you have a clear desk policy?
- Ensure confidential conversations cannot be overheard
- Keep your password secret
- Ensure information is transported securely



# Principle 7 (*Organisational*)

## Protected by appropriate security

**Your organisation should have ...**

- Good information management practices
- Guidelines on IT security
- Staff training
- Confidentiality clause in employment contracts
- Procedure for access to personal data
- A disposal policy/procedure for confidential information
- Confidentiality contracts with third parties

e.g. archiving companies, cleaners,  
temporary staff, outside contractors



# Principle 8

## Not transferred outside the European Economic Area (EEA) without adequate protection

- If sending personal information outside the EEA ensure consent is obtained and it is adequately protected
- Be careful about putting personal information on websites - gain consent first
- Check where your information is going e.g. where are your suppliers based?



The EEA comprises: EU Member States plus Iceland, Liechtenstein and Norway

# To sum up, remember that information must be:

**Held securely and confidentially**

**Obtained fairly and efficiently**

**Recorded accurately and reliably**

**Used effectively and ethically**

**Shared appropriately and lawfully**



# For further information contact...



**Your Data Protection Officer**



**Your Caldicott Guardian**



**The Information Commissioner's website:**

<http://www.ico.gov.uk>



**The Caldicott website:**

<http://www.dh.gov.uk>

