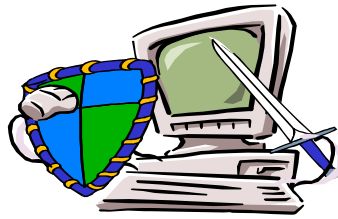


Protecting Privacy



**Creating a safe environment
for working with personal information**

Staff Information Leaflet

The Data Protection Act 1998 came into force in March 2000 and relates to personal information about living individuals, in whatever format. Every organisation that processes personal information must notify under the Act and failure to do so can result in a substantial fine. The Data Protection Act is the law and breaches of confidentiality can result in criminal proceedings, usually for the organisation but in some cases, the individual. Dame Fiona Caldicott also prepared a report recommending action to be taken to safe guard patient confidentiality for the NHS called the Caldicott Report. There are 8 Data Protection Principles, and 6 Caldicott Principles for handling personal identifiable information. The Data Protection Act is the legal arm and the Caldicott principles are the guidelines to which the NHS works.

WHAT INFORMATION DO WE SHARE AND WHY?

The information entrusted to us is very important. It is personal and sometimes very sensitive and the public should feel confident that we keep this information safe. Patient confidentiality underpins the whole structure of the NHS and remains the highest priority, and improvements are continually being made to build upon this. The NHS is made up of a team of dedicated professionals and so that patients can have access to the wide range of expertise in this team, their information will normally be shared with others involved in the treatment or investigation of their medical problem. The NHS is using new technology to help deliver better patient care which means health records can now be stored and shared electronically but also securely.

WHO HAS ACCESS?

Doctors, nurses and other health professionals would need access to records, but this is on a strict need to know basis. Only those involved in the treatment and care of that patient would need access. Secretaries, receptionists, and other clerical staff will need limited access in order to carry out administrative tasks such as booking appointments and communicating with patients and other sections of the NHS.



*.... is there
another
way his identity
can be known?*

WHAT ELSE HAPPENS TO THE INFORMATION?

Some of this information may also be shared for purposes other than the patient's own health care. This leaflet has been prepared to help explain who we may share the information with, and under what circumstances. The information is anonymous wherever possible but if the patient has any concerns regarding the sharing of this information they have the right to refuse to allow all, or some, of their information being used.

Teaching and training of healthcare professionals



Training is very important to ensure that healthcare professionals have the skills and knowledge to provide the healthcare services of the future. Wherever possible data will be anonymised, (no personal information will be included) but this is not possible for training carried out as part of clinic activities. Patients have the right to refuse to allow identifiable information to be used for teaching and training purposes and this will not affect their immediate care in any way. However, it may limit the development of future staff whose services they may require.

To help plan future social care

In order to offer a complete care package patient information may sometimes be shared with Social Services or other non-NHS agencies. This will only be with the patient's consent and they have the right to refuse, but such refusal will limit the ability to arrange any ongoing care they may need, once their NHS care is completed.



Funding local health services



Limited information must be transferred to obtain payment for patient health services from the appropriate funding body (e.g. NHS,

private insurance). This information will be restricted to the minimum necessary to secure those payments.

Health research projects



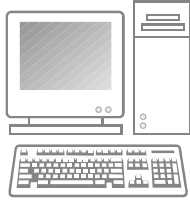
Some medical research will directly involve patients. For example, taking part in a clinical trial (where a new treatment is being tried). If a patient is asked to participate in a trial, it will be fully explained, and their express consent required. If the patient does not consent, they will not be included in the trial, and this will not affect the standard treatment offered to them. Other research may not involve the patient directly, but may rely upon access to their clinical information. Some databases, e.g. the Cancer Registry, are set up for national research in the fight against diseases such as cancer. Research work, is guided by the Medical Research Council document "*Personal Information in Medical Research*". This represents the working standard for the use of patient information for research purposes. It sets out when and how researchers need to obtain specific consent to access information. The patient has the right to refuse access to their information for research. Researchers who have access to clinical information must protect confidentiality, and ensure that information stored for any research project is made anonymous, wherever this is possible. They must also present their research proposals before an Ethics Committee to check that their research is appropriate and worthwhile, and to check that data protection issues have been considered.

To help plan future health services

We need to be able to plan ahead so that the care provided is of the highest standard. It is important that health services should regularly review the quality of care they provide. We need to investigate how we provide treatment and care and this means getting information from patient records or sending out questionnaires. Where treatment is provided across a number of hospitals, it is necessary to share data using centralised disease registers in order to assess the overall treatment delivered. Some clinical information is therefore routinely transferred into approved registers, but access to this information is strictly controlled. When analysing the results of audits anonymised and summary information is used, not individual patient information.



Managing the data



We need to move electronic information between systems, extracting the data and modifying it for the next system. Occasionally, tests will need to be made on the data to check that it has been transferred correctly. This will only be done under carefully controlled conditions and all employees and contractors will be under strict contractual obligations to protect confidentiality. Real patient identifiable information should not be used in demonstrations or testing of systems

WHAT ELSE DO WE DO WITH THE INFORMATION?

The NHS has a statutory obligation to notify the government of certain infectious diseases for public health purposes, e.g. measles, mumps, meningitis, tuberculosis, **but not AIDS**. Births and deaths must also be notified.

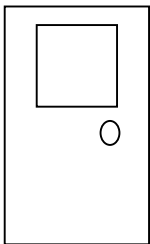
Limited information is shared with Health Authorities to assist with the organisation of national public health programmes, e.g. breast screening, cervical smear tests, and childhood immunisation.

A Court of Law can insist that medical information be disclosed to them.

Solicitors sometimes request medical reports but these requests must be accompanied by the signed consent of the patient. Third party information in the record will be withheld unless the third party has also given written consent.

WHAT YOU CAN DO TO HELP

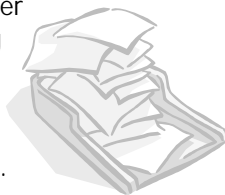
Room Security



Do not leave your room unattended and unlocked. If your room can be locked without compromising patient care, for example, where the patient information is unlikely to be needed by non-keyholders, then it should be locked away.

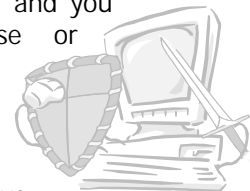
Patient information left lying around

When working with personal information, only have the minimum necessary to carry out your work. All other related documents and papers should be locked away - shred if no longer needed. Do not put in the waste paper bins or general recycling bins. Some organisations have a confidential waste destruction programme. Ask if you are not sure.



Information held on computers

Passwords are the keys that provide access to information and you must never disclose or share your password with anyone, even if they are in a more senior position to yourself. If you have personal information on your computer, ensure that it is stored in a secure way with password protection. Remember to log-off when you have finished with your computer.



Faxing patient information

When faxing confidential information, use a Safe Haven fax machine wherever possible. A designated Safe Haven fax machine is a machine where confidential information can be sent safely as procedures are in place at the other end to safeguard its security. If this is not possible, follow the guidelines for faxing manual faxes.



Transferring information manually

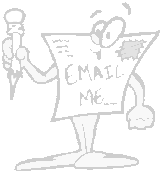
When you are transferring personal information make sure that it is properly addressed and marked "CONFIDENTIAL". Do not take personal notebooks or pocket books away from your place of work. Remember to hand them back if you no longer need them for your job. Contact your Medical Records department or Practice



Manager if you have any specific questions regarding the transfer of information.

E-mail

Remember, you are responsible for the contents of your e-mails. Ensure that the content is not sexually or racially offensive, or otherwise illegal. Do not send patient information via the Internet, as this is not a secure system. (Use only addresses that end in .nhs.uk)



Indiscreet conversations



Ensure that you cannot be overheard when discussing confidential information, either over the phone or with colleagues. Take care not to discuss personal information in hallways, staircases or any public place where you may be overheard. If you do not need to mention a person by name, then don't. If you have an answer phone make sure that recorded messages cannot be overheard when you play them back. If you have a call you are unsure about, confirm the caller's identity or ring back.

ACCESS TO INFORMATION

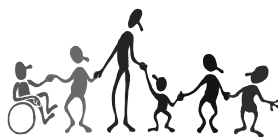
Patients and members of the public are allowed to see their medical records under the Data Protection Act 1998. Requests must be responded to within 40 days and should be in writing to the Medical Records Office (if applying to a hospital) or their own GP. There is a duty to keep medical records up to date. If anything has been added to the record that is factually incorrect, the patient has the right to have it amended. The patient can also apply for compensation for any distress caused by the inclusion of factually incorrect information.

If you wish to discuss issues that you feel should be addressed, or if you have any examples of good practice that you would like to share, please contact: **Pauline Evans, Caldicott Support Officer, Wirral Health Informatics Service, Admin Block, St Catherine's Hospital, Church Road, Birkenhead CH42 0LQ ☎ 0151 651 0011 x 226**

The Caldicott Principles

1. Justify the purpose
2. Do not use patient identifiable information unless it is absolutely necessary
3. Use the minimum necessary patient identifiable information
4. Access to patient identifiable information should be restricted on a strict need to know basis
5. Everyone should be aware of their responsibilities
6. Everyone should understand and comply with the law

Wirral **NHS**



Working to keep your personal information safe

The Data Protection Act 1998

1. Personal data shall be processed fairly and lawfully
2. Personal data shall be obtained only for one or more specified lawful purposes
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
4. Personal data shall be accurate and, where necessary, kept up to date
5. Personal data processed for any purpose or purposes shall not be kept longer than is necessary for that purpose or those purposes
6. Personal data shall be processed in accordance with the rights of data subjects under this Act, including the right to access their own records
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss
8. Data shall not be transferred outside of the European Economic Area

How much do you know?

1. What is a Safe haven fax machine?

- a) a fax machine situated in a village in Scotland
- b) a fax machine situated in an open office area
- c) a fax machine where you can send confidential information where you know procedures are in place to ensure its security

2. What piece of legislation protects personal data?

- a) Criminal Justice and Police Act 2001
- b) Environment and Safety Act 1998
- c) Data Protection Act 1998

3. A Caldicott Guardian is:

- a) columnist in a national newspaper
- b) a type of protective footwear
- c) an appointed senior person who is responsible for overseeing access to patient information

4. Who is an unauthorised person?

- a) everyone except the doctor
- b) everyone except the patient
- c) anyone who doesn't need to know

5. How many Caldicott Principles are there

- a) 10
- b) 8
- c) 6

6. It is OK for your password to be shared with

- a) your colleagues in your office
- b) your boss
- c) your password should never be shared with anyone

7. When you are going to leave your computer unattended you should always:

- a) cover up
- b) shut down
- c) log off

ANSWERS ON THE BACK PAGE.....

1. Whilst Safe Haven might be a very pretty “get away from it” sort of place in Scotland, the correct answer here is c). A fax machine sited in an open office can never be described as a Safehaven fax machine.

If you are in doubt when faxing confidential information, always telephone first. If you are not sure, don't forget to follow the guidelines for the safe transmission of manual faxes.

2. Data Protection Act 1998 protects the way personal information is processed – in whatever form; written, verbal, visual. This includes: telephones, answering machines, CCTV, printers, notice boards, disks, computer screens, audio tapes, photocopiers, lists of names and addresses, etc.
3. A Caldicott Guardian is a senior health professional, or a member of the management board, for each organisation. The Guardian is responsible for agreeing and reviewing protocols governing the disclosure of patient identifiable information across organisational boundaries. Do you know the Caldicott Guardian for your organisation?
4. An unauthorised person is simply a person who does not need to know the information. Caldicott Principle 4 states that access should be restricted on a strict “need to know” basis, and even then it is restricted only to the parts of information needed. Do not assume that your work colleagues are authorised to see the same information that you are, even if they are in a more senior position.
5. There are 6 Caldicott Principles and 8 Data Protection Principles. They work hand in hand, Data Protection is the legal arm, and the Caldicott Principles are the guidelines to which the NHS works.
6. Passwords are the keys that provide access to information and your password should never be shared with anyone under any circumstances. You will be held responsible for any actions associated with your password.
7. Never leave a computer logged onto a system and unprotected. Always protect the system (e.g. log off or use a password-protected screen saver) when you have stopped using it for a period. Always log off when you have finished.