The Mid Yorkshire Hospitals NHS
NHS Trust

Confidentiality

What you need to know!!

A guide for trust employees in confidentiality and information security

Contents **Page**

Purpose of this booklet	1
What is confidential information?	2
Information Governance	3
Confidentiality	3
IT Security	5
Guidance on the appropriate use of Smartcards	6
IT Policies	7
Disclosure of Patient Information	7
Information Sharing	7
Consent	8
Data Protection Act 1998	9
Caldicott	10
Records Management	11
Freedom of Information Act	11
Local Confidentiality Arrangements	12
Further reading	12

Purpose of this booklet

The purpose of this booklet is to clarify the principles that govern the use of personal identifiable information and to ensure that good practice is adhered to. We are all responsible for the security and confidentiality of information within the Trust and it is only by knowing what your responsibilities are that you will know how to deal with situations appropriately.

All employees working in the NHS are bound by a legal duty of confidentiality to protect personal information they may come into contact with during the course of their work. This is not just a requirement within their clinical registrations or contractual responsibilities but also a requirement within the Data Protection Act 1998. This means that **all** employees are obliged to keep any electronic or paper based person identifiable information strictly confidential e.g. patient and employee records, patient referral letters, discharge summaries. It should be noted that employees also come into contact with non-person identifiable information which should also be treated with the same degree of care e.g. contractual information.

The Trust Corporate Information Governance Steering Group (CIGSG) considers and monitors all issues surrounding confidentiality and information security, and reports back to the Trust board. The Trust also has a confidentiality and IM&T information security service which, as well as following a comprehensive work programme, has a helpdesk, and offers support, guidance and training to all staff. The helpdesk can be contacted on x 5000

What is Confidential Information?

Confidential information can be anything that relates to patients, staff, their family or friends, however stored. This information may be held on paper, CD, computer file or printout, video, photograph or even heard by word of mouth. It includes information stored on portable devices such as laptops, mobile phones and digital cameras. It can take many forms including medical notes, audits, employee records, occupational health records etc.

Information is an extremely valuable asset to the Trust. Information held concerning patients is personal and can be highly sensitive. Information held within the Trust can affect you personally e.g. personnel files and information is also held about the Trust itself e.g. financial details.

The effect of any loss of this information could be dramatic!

You should consider all information to be sensitive, the same standards should be applied to any information you come into contact with.

All NHS bodies and those carrying out functions on behalf of the NHS have a Common Law Duty of Confidentiality to patients and a duty to maintain professional ethical standards of confidentiality. Personal information given or received in confidence for one purpose should not be used for a different purpose or passed to anyone else for a different purpose, unless there are exceptional circumstances or the consent of the provider of the information is obtained. Information kept must be accurate and up to date and should be available to the right people, at the right time.

Information Security is the responsibility of everyone in the Trust.

Although there is no complete defence against something going wrong, improved security and staff awareness will reduce the chances of loss or will help recovery from any loss suffered. Staff involvement also helps new and improved procedures to be introduced where necessary.

The Trust Information Security Policy is available on the intranet.

Information Governance

There is a Corporate Information Governance Steering Group (CIGSG) which meets regularly to oversee confidentiality and information security issues. It is made up of the SIRO, Caldicott Guardian, Associate Director of IT, the Information Governance Officer and a representative range of staff from both clinical and information management backgrounds. The Group ensures that all information used in the Trust is managed carefully, responsibly, within current law and with due regard to considerations of privacy, and that all staff are made aware of their obligations in this area.

You can contact any member of the Group with Information Governance questions.

	Based at
Dr Ian Wilson (Caldicott Guardian)	Trust HQ, Pind
Bob Chadwick (SIRO)	Trust HQ, Pind
James Rawlinson	DDH
Jenny Johnson	DDH
Lewis Judge	Trust HQ, Pind
Ellie Valentine	Trust HQ, Pind
Lesley Barret	DDH
Liz Hayes	Trust HQ, Pind
Paul Jefferson	Trust HQ, Pind
Mick Lawton (IG Officer)	DDH/THIS

Confidentiality

The Health Service holds large amounts of confidential information and it is our responsibility to safeguard that confidentiality. The information we hold belongs to the individual people it concerns and we must ensure that information cannot be seen or changed by anyone that does not have the right to see it.

Treat other people's information in a way that you yourself would like yours to be treated.

Telephone – If a request for information is made by telephone always try to check the identity of the caller and check whether they are entitled to the information they are requesting. Take a number, verify it independently and call back if necessary.

Talk – Always ensure that you do not talk about patients in public places (this includes internal public areas such as the dining rooms, corridors and Trust transport) or where you can be overheard. Only give out information regarding patients or staff to persons who "need to know" or who can justify why they require the information.

Fax safely – Patient identifiable information should only be faxed following the safe faxing guidelines (a copy of these should be positioned near every fax machine – if not please contact the Information Governance Service on x 5000).

Mail – All envelopes containing confidential information should be clearly marked 'Private and Confidential' and fully addressed. Mark the reverse with a return name and address if required. Follow the Trust's Document Control Guidance and print all private, confidential or sensitive documents on pink paper.

E-mail – You can now email confidential data between Mid Yorks email accounts without password protecting it. External emails of confidential data must be be password protected and sent and received by NHS Net/ Mail. Read the Trusts Email policy for further details.

Removable Storage Devices - must be encrypted and password protected and you must only use Trust approved devices.

Keeping information safe – Always ensure that any medical records or confidential information is not left unattended where it could be accessed inappropriately, even for a short time. Paper-based confidential information should always be kept locked away and preferably in a room that is locked when unattended.

Disposal of confidential information – Always use 'Confidential Waste' sacks/ cross cut shredders. Keep the waste in a secure place until it can be collected for secure disposal.

I T Security

Computers

- Always lock your workstation if you are leaving it (CTRL+ALT+DEL).
- Never divulge your password to anyone and do not write it down.
- Do not allow any one else access whilst you are logged in.
- Ensure that computer screens, or other displays of information, cannot be seen by the general public or unauthorised staff.
- Avoid keeping confidential information on your hard drive, your computer could be stolen – ensure that it is always saved to the network (if you need further advice on this ring the IT Service Desk on x5000).
- Do not divulge information to someone who has no right to that information.
- Do not attempt to access any part of the system that you are not authorised to.
- Authorised users must not access information inappropriately e.g. to find a colleagues birthday or address.
- If you suspect you have a virus on your computer or need software loading to it contact the IT Service Desk on x5000 immediately.
- Only use Trust authorised software.

Internet – The Trust encourages appropriate use of the internet as a tool to provide information to assist you in your work. The Trust has no objection to staff making modest personal use of the Internet in their own time although certain restrictions apply. Unauthorised material includes illegal or unauthorised software, any material of a sexual or pornographic nature, racist material etc.

Internet activity is monitored centrally by the Trust and users should be aware that access can be traced back to an individual user. Misuse of the internet may result in access being denied and disciplinary action will be taken by the Trust which could lead to the dismissal of the individuals concerned. (Please read the Internet Use Policy on the Trusts intranet site for more information).

Intranet – The intranet is restricted to people who are connected to the Trust's network. It is a site used to share information across the Trust. There is a wealth of information on the intranet relating to each department throughout the Trust.

Guidance on appropriate use of smartcards

If you are issued with a Smartcard and Passcode to fulfil your role in the Trust, you must:

- Carry it whenever you may need to access the NHS Care Records Service (NCRS).
- Keep it safe and secure. Treat your Smartcard like your credit or debit card.
- Never tell, share or write down your Passcode.
- Never allow anyone to use your Smartcard - checks on access will be made and you will be held responsible for all patient data recorded and accessed using your Smartcard.
- Never leave your Smartcard unattended.
- Report the loss, theft or damage of your Smartcard immediately to your line manager and local Registration Authority Team.
- Smartcard sharing is considered misconduct and may result in disciplinary action.

If you have further questions please speak to the Trust's Registration Authority Team. Contact details can be found in the internal directory.

IT Policies

There are Trust policies covering internet access, e-mail, information security and network access which are available on the Trust intranet. **You should make sure you have read and understood these policies.**

Disclosure of patient information

Patients have a right to expect that information about them will be held in confidence. Without assurances about confidentiality patients may be reluctant to provide information. Patients should understand what may be disclosed, the reasons for the disclosure and be given the opportunity to withhold permission for disclosure. You must respect requests by patients that information should not be disclosed to third parties except in exceptional circumstances e.g. where the health or safety of others would otherwise be at serious risk.

If you decide to disclose confidential information without consent then you must be prepared to explain and justify your decision and equally you must be prepared to explain and justify your decision not to disclose information. You must keep records of disclosure decisions and the reasoning behind them.

Many improper disclosures are unintentional. Make sure you cannot be overheard when you discuss patients, make sure that you put paper information away and do not leave information on screens. You should anonymise confidential information whenever possible.

Information sharing

Sharing information is sometimes essential but we must always comply with the law. Only share information that identifies a patient for care and quality checks on that care, unless the patient consents, the law requires it or the information is anonymised. Information should only be shared in appropriate circumstances.

- Always check the member of staff is who they say they are before giving them any information.
- Share only as much identifiable information as people need to know or are entitled to know.

- Take opportunities to discuss with patients how their information will be shared.
- Ensure patient information is accurate and up to date before it is shared.
- If in doubt discuss your concerns with a senior colleague or IG officer.
- There is an Interagency Information Sharing Protocol which is a framework for sharing information that has been signed up to by health and local authority organisations throughout Yorkshire, this has been developed in recognition of the increasing need to work together across organisations. A copy of this is available from the Information Governance Officer and on the Trust intranet.

Consent

The Trust is obliged to ensure that the information that we take from patients is held and used within the legal framework of the Data Protection Act 1998, the Public Records Act 1958 and complies with the Caldicott Principles.

It is very important that reasonable efforts are made to ensure that patients understand how their information is to be used to support their healthcare and that they have no objections to its use. When this is done effectively consent can be implied providing that "need-to-know" principles and data protection principles are enforced.

When patients consent to disclosure of information about them you must make sure they understand what will be disclosed, the reasons for the disclosure and the likely consequences.

A patient's refusal to allow information sharing with other health professionals may compromise the patient's safety but if this is an informed decision by a competent person it should be respected. However, every effort should be made to explain to the individual the consequences for care and planning but the final decision rests with the individual.

The Trust leaflet 'Keeping and protecting information about you and your care' is available throughout the Trust to give patients more information.

Data protection act 1998

The Data Protection Act applies to personal data which is held in ANY formal system whether manual or computerised. There are 8 principles of good practice which all staff need to be aware of.

Information must be:

1. **Fairly and lawfully processed** – inform people why you are collecting their information and what you are going to do with it and who you may share it with. Be open, honest and clear.
2. **Processed for limited purposes** – only use personal information for the purpose for which it was obtained. Only share information if you are certain it is appropriate and necessary to do so.
3. **Adequate, relevant and not excessive** – only collect and keep the information you require. Be concise and clear.
4. **Accurate and kept up-to-date** – take care inputting information and always confirm details with patients. Check existing records thoroughly before creating new records.
5. **Not kept longer than necessary** – dispose of information carefully and follow retention guidelines.
6. **Processed in accordance with the data subject's rights** – prevent processing for any reasons other than those for which the data was collected. Allow individuals access to information through the subject access request system.
7. **Secure** – always keep confidential papers locked away, keep your password secret, ensure you cannot be overheard and ensure information is transported securely.
8. **Not transferred to countries out of the EEA without adequate protection** – make sure that consent is obtained and check where the information is going.

Caldicott

Caldicott is a report named after the author, Dame Fiona Caldicott, and relates to patient identifiable information within the NHS. Complying with Caldicott reduces the risk of breach of confidentiality and breaking the law. It is the responsibility of the Caldicott Guardian to oversee that the organisation is adhering to Caldicott guidelines and make final decisions on issues regarding confidentiality.

The seven Caldicott principles are:

1. **Justify the purpose for using confidential information.**
   Can you justify why you are accessing this information?
2. **Only use information when absolutely necessary.**
   Do you really need to use patient identifiable information for your purpose - could it be anonymised?
3. **Use the minimum that is required.**
   Have you considered each item of information and can you justify its use for the given function to be carried out?
4. **Access should be on a 'need-to-know' basis.**
   Do you really need to see the whole record or just a relevant section of it? Do you really need to see the information at all?
5. **Everyone must understand their responsibilities.**
   Have you had enough training to be able to fulfil your responsibilities and obligations? Are you happy that you know what they are?
6. **Understand and comply with the law – common law duty of confidence/Data Protection Act (1998).**
   Are you aware of the principles of law surrounding patient identifiable information?
7. **The Duty to share confidential data can be as important as the duty to respect service user confidentiality.**

NHS Care Records Guarantee

The care record guarantee sets out the commitment of the NHS in its use of patient information as the health service in England moves towards a national electronic system - the NHS care records service. A link to the NHS care record guarantee can be found on the intranet.

Records management

Records are a valuable resource because of the information they contain. That information is only usable if it is correctly recorded in the first place, is updated appropriately, and is easily accessible when it is needed.

All healthcare workers are responsible for maintaining clinical records and ensuring that they are secure and obtainable and anyone who creates or makes use of a record is responsible for its safekeeping.

Information is essential to the delivery of high quality, evidence based health care on a day to day basis and an effective records management service ensures that such information is properly managed and is available.

Every department has a procedure for managing records – it is your responsibility to familiarise yourself with this.

For specific advice on retention and disposal of records ask your line manager. The NHS records management code of practice sets out the legal obligations for all NHS bodies to keep proper records and provides guidelines on good practice. It also sets out the minimum time records need to be kept.

There is a Trust policy for the management of Health records which can be found on the Trust's Intranet.

Freedom of information Act 2000

Under the Freedom of Information Act 2000 members of the public have the right to request any information held by the Trust (other than where exceptions apply).

The Trusts Publication Scheme gives a description of information that the Trust makes available to the Public and can be found on the Trusts web site www.midyorks.nhs.uk

All Freedom of Information requests from the Public should be forwarded to the Trust Freed om of Information (FOI) Lead - FOI@midyorks.nhs.uk

The Freedom of Information Act 2000 does not contravene the Data Protection Act 1998 as no person identifiable information can be released under this Act.

Local Confidentiality Arrangements

Mid Yorkshire staff should ensure that they are fully aware of any specific local procedures with respect to issues of confidentiality in the area they work in.

Further reading

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf

Confidentiality policy statement and supporting guidance:
The Mid Yorkshire Hospitals NHS Trust

Remember everyone is responsible
for confidentiality and information security

For further information on anything you have seen in this leaflet please seek advice by contacting the Confidentiality and IM&T Security Helpdesk

x5000

DOCUMENT CONTROL

Author	Information Governance Officer
Contributors	Pennine Care Trust, C&H HIS
Version	4.0
Date of Production	June 2015
Date due for revision	June 2018
Post responsible for revision	Information Governance Officer
Primary Circulation list	All Mid Yorkshire Trust Employees
Restrictions	**None**

We are committed to providing high quality care. If you have a suggestion, comment, complaint or appreciation about the care you have received, or if you need this leaflet in another format please contact the Patient Advice and Liaison Service on: 01924 542972 or email: pals@midyorks.nhs.uk

To contact any of our hospitals call: 0844 811 8110
To book or change an appointment call: 0844 822 0022

997k
Updated June 2015
Review Date 2018

SMOKE FREE
hospital

cleanyourhands© campaign

Design: The Mid Yorkshire Hospitals NHS Trust - design and print dept