The Mid Yorkshire Hospitals NHS
NHS Trust

CONFIDENTIALITY POLICY STATEMENT AND SUPPORTING GUIDANCE

Document control

Numbered Document: CORP030v5.0
Author: Information Governance Service, THIS
Lead Director: Director of Finance
Version Number: 5.0
Ratified at: CEG 15 March 2017
Date of publication on MY Intranet: 31 March 2017
Date Due for Revision: November 2019
Post Responsible for Revision: Information Governance Service, THIS
Equality Impact Assessment: Attached
Restrictions: None
Total Pages: 30

Review and Amendment Log

Version No	Type of Change	Date	Description of change
V1	Review and update		Produced by Confidentiality and IM&T Security Service
V2	Review and update		Updated by Confidentiality and IM&T Security Service
V3	Review and update		Updated by Information Governance Team (THIS)
V4	Review and update		Updated by Information Governance Team (THIS)
V5	Review and update to include use of text messages and record keeping best practice	October 2016	Updated by Information Governance Team (THIS)

Confidentiality Policy Statement

1 Purpose

The purpose of this Policy Statement is to ensure that everyone working within Mid Yorkshire Hospitals NHS Trust is aware of their responsibilities when using confidential information.

The principle underpinning this policy statement is that no employee shall misuse any information or allow others to do so.

The policy statement has been written to support staff in compliance with the following legal requirements and best practice guidance:-

- Data Protection Act 1998 (DPA)
- Human Rights Act 1998
- Common Law Duty of Confidentiality
- The Caldicott Report 1997 and Caldicott 2
- The NHS Confidentiality Code of Conduct

All departments of the NHS need to establish working practices that effectively deliver the level of confidentiality that is required by law, ethics and policy statement. The objective must be continuous improvement.

2 Supporting Guidance

This policy statement is supported by guidance for staff which:

a. Introduces the concept of confidentiality and the duty of confidence
b. Demonstrates the practical safeguards that should be put into place
c. Provides a high level description of the main legal requirements and should be read in conjunction with the Confidentiality Policy Statement : Guidance

Annual, Mandatory Training in Information Governance is provided to all staff at induction and routinely via e learning, mandatory training sessions and literature.

3 The Policy Statement

This Policy statement applies to all personal and sensitive personal data, whether written, computerised, visual, audio or held in the memory of a member of staff. It applies equally to staff on permanent, temporary or voluntary contracts.

Health care professionals and the staff that support them hold information about people that may be private and sensitive. Patient information is collected to provide care and treatment to individuals and generally must not be used for other purposes without their consent. In the same way, information about staff that is processed for the purpose of their employment is confidential. Confidentiality should only be breached in exceptional circumstances and with appropriate justification and be fully documented.

Key Principles

- When you are responsible for confidential information you must ensure that the information is effectively protected against improper disclosure when it is used, received, stored, transmitted, disclosed or disposed of;
- Access to confidential information should always be on a need-to-know basis
- Every effort should be made to inform patients how their information is going to be used and who it will be shared with and why it may be shared
- When patients consent to disclosure of information about them, they must be made aware of what is being disclosed, the reason it is being disclosed and the likely consequences of that disclosure
- If the patient withholds consent, or if consent cannot be obtained, disclosures may be made only where:
    - They can be justified in the public interest (usually where disclosure is essential to protect someone from the risk of significant harm)
    - They are required by law or by a court order
- Only as much information as is needed for the purpose must be disclosed
- Recipients of disclosed information must respect that it is given to them in confidence
- If the decision is taken to disclose information, that decision must be justified and documented.
- Any doubts at all about disclosure must be discussed with either your line manager or the Information Governance Service.

4 Contract of Employment

Your contract of employment includes a commitment to confidentiality. Breaches of confidentiality could be regarded as gross misconduct and may result in serious disciplinary action up to and including dismissal.

5 Duties (Roles & Responsibilities)

Chief Executive

The Chief Executive is responsible for ensuring that the necessary support and resources are available for the effective implementation of the Confidentiality Policy.

The Information Governance Group

The Corporate Information Governance Steering Group (CIGSG) are responsible for the review and approval of the Confidentiality Policy.

Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) has organisational responsibility for all aspects of Information Governance, including the responsibility for ensuring that the Trust has appropriate systems and policies in place to maintain the security and integrity of the Trusts information.

Caldicott Guardian

Dr Ian Wilson is the Caldicott Guardian.

The Mid Yorkshire Hospitals NHS Trust

CONFIDENTIALITY POLICY STATEMENT: GUIDANCE

CONTENTS:

Summary

The aim of this guidance is to support the Confidentiality Policy statement and to promote good practice for all members of staff in the protection and use of personal and sensitive personal data. Also to ensure that the requirements of the Data Protection Act 1998 and other relevant legislation are adhered to and recommendations of the Caldicott report and the NHS Confidentiality Code of Practice are understood. An overview of relevant legislation and guidance is provided in Part 3

The guidance ensures that staff understand the correct procedure for handling information so that they do not inadvertently breach confidentiality.

The guidance aims to do the following:

a. To introduce the concept of confidentiality and the duty of confidence;
b. To demonstrate the practical safeguards that should be put into place;
c. To provide a high level description of the main legal requirements.

The objective of the policy is that of continuous improvement.

1. Part One – Statement of Confidentiality

2. Part Two – Confidentiality: the practical application

3. Part Three – an explanation of the legal implications and the framework that has been put in place to support these

Part One - Confidentiality

1. Statement of Confidentiality

1.1 Respect for confidentiality is an essential requirement for the preservation of trust between patients and health and social care professionals. Without assurances about confidentiality, patients may be reluctant to provide the information that is needed to deliver appropriate levels of care.

1.2 Health and social care professionals hold information about patients that is both private and sensitive. This information is collected to provide care and treatment to individuals and generally must not be used for other purposes without the individual's knowledge and consent.

1.3 Confidentiality should only be breached in exceptional circumstances and with appropriate justification. When a health or social care professional can justify that information should be released they should act promptly to disclose all relevant information. This is often essential to the best interests of the patient, or to safeguard the well-being of others. Any such breaches should be fully documented giving justification for the breach.

1.4 The organisation holds personal information about each staff member and this information must be treated with the same level of confidentiality with which patient information is held.

2. Duty of Confidence

2.1 A duty of confidence arises when one person discloses information to another (e.g. patient to clinician) in circumstances where it is reasonable to expect that the information will be held in confidence. The obligation to confidentiality is:

- a legal obligation that is derived from case law;
- a requirement established within professional codes of conduct; and
- included within employment contracts as a specific requirement linked to disciplinary procedures.

2.2 Patients entrust us with, or allow us to gather, sensitive information relating to their health and other matters as part of their seeking treatment and advice. They do so in confidence and they have the legitimate expectation that staff will respect their privacy and act appropriately. In some circumstances patients may lack the competence to extend this trust, or may be unconscious, but this does not diminish the duty of confidence. It is essential, if the legal requirements are to be met and the trust of patients is to be retained, that the Trust provides, and is seen to provide, a confidential service.

2.3 Children are due the same level of confidentiality as an adult, if they are deemed to be competent to make decisions about their own healthcare.

2.4 For a child to be competent they must fully understand any treatment that is proposed and what the outcomes are of that treatment are and should be encouraged to involve their parents or another suitable adult in any decisions made. Only a Health Care Professional may decide if a child is competent

2.5 Information that can identify individual patients, must not be used or disclosed for purposes other than healthcare without the individual's explicit consent, some other legal basis, or where there is a robust public interest or legal justification to do so. In contrast, anonymised information is not confidential and may be used with relatively few constraints.

3. Using and disclosing confidential patient information

3.1 Patients should be informed about

- The use and disclosure of the information associated with their healthcare[1]; and
- The choices that they have and the implications of choosing to limit how that information may be used or shared; and the decision should be documented

3.2 Consent to disclosure can be taken to be implied when needed to provide healthcare. However, opportunities to check that patients understand what may happen should be taken.

3.3 It is extremely important that patients are made aware of information sharing that must take place in order to provide them with high quality care. Whilst patients may understand that information needs to be shared between healthcare professionals they may not be aware of sharing between different organisations involved in the provision of their healthcare. Efforts must be made to inform them of everyone who will be sharing their information. This is particularly important where disclosure extends to non-NHS bodies. Equally, clinical governance and clinical audits, which are wholly proper components of healthcare provision, might not be obvious to patients and use of information in this way should be drawn to their attention.

3.4 Patients generally have the right to object to the use and disclosure of their confidential information and need to be made aware of this right. Patients need to be made aware that by not consenting to certain disclosures they may be compromising their care. Clinicians cannot usually treat patients safely, nor provide continuity of care, without having relevant information about a patient's condition and medical history. If in doubt, contact the Information Governance Team on x5000.

4. Ethical standards

4.1 The disclosure and use of confidential patient information needs to be both lawful and ethical. The law provides a minimum standard that does not always reflect the appropriate higher ethical standards that the government and the professional regulatory bodies require.

5. Protecting information

It is essential that personal information be effectively protected against improper disclosure at all times. This applies to information held both electronically and on paper.

[1] Heathcare purposes are defined as including all activities that directly contribute to the diagnosis, care and treatment of an individual and the audit/assurance of the quality of the heathcare provided. They do not include research, teaching, financial audit or other management activities.

Many improper disclosures are unintentional. All staff should ensure that the following principles are adhered to:-

- All reasonable steps should be taken to ensure that consultations with patients are conducted confidentially;
- Specific cases should never be discussed where it is possible that you could be overheard;
- Patients' records, either on paper or on screen, should not be left where they can be seen by any unauthorised person;
- Information must be stored securely;
- All information held on any portable Trust supported computer or storage devices or media e.g. laptop computer, memory stick, DVD etc must be encrypted to 256 Advanced Encryption Standard (AES);
- If there is a business need to hold any confidential information on a portable non encrypted Trust supported or computer storage device, then this must be approved by your Line Manager or the Trusts SIRO;
- Staff must not look up their own records or those of another person i.e. family member, even when they have the consent of that person to look at their records for any purpose i.e. to view test results, confirm appointments etc.
- When you are responsible for confidential information you must ensure that the information is effectively protected against improper disclosure when it is received, stored, transmitted, disclosed or disposed of;
- Access to confidential information should be on a strict need-to-know basis;
- Every effort should be made to inform patients how their information is going to be used and who it will be shared with and why it may be shared;
- When patients consent to disclosure of information about them, they must be made aware of what is being disclosed, the reason it is being disclosed and the likely consequences of that disclosure;
- If the patient withholds consent, or if consent cannot be obtained, disclosures may be made only where:
  - They can be justified in the public interest (usually where disclosure is essential to protect someone from the risk of significant harm)
  - They are required by law or by a court order
- Only as much information as is needed for the purpose must be disclosed;
- Recipients of disclosed information must respect it is given to them in confidence;
- If the decision is taken to disclose information, that decision must be justified and documented;
- All non consented disclosures of patient information must be approved by the Caldicott Guardian unless it is a matter of life and death or there is the possibility of imminent serious or potential serious harm to a person or persons;
- All non consented disclosures of staff information must be approved by the Senior Information Risk Owner (SIRO) unless it is a matter of life and death or there is the possibility of imminent serious or potential serious harm to a person or persons;
- Any doubts at all about disclosure must be discussed with either your line manager or the Information Governance Team on 0845 1272600.

Part Two – Confidentiality: The Practical Application

1. Definitions

1.1 What is patient identifiable information?

"All items of information which relate to an attribute of an individual should be treated as potentially capable of identifying patients and hence should be appropriately protected to safeguard confidentiality"
Caldicott Committee: Report on the review of patient identifiable information, 1997

These items include:

Surname
Initials
Date of Birth
Postcode
Sex
National Insurance Number
Forename
Address
Telephone Number
Occupation
NHS or Staff number
Ethnic Group

1.2 What is staff identifiable information?

All items of information which relate to staff should be treated as potentially capable of identifying staff and hence should be appropriately protected to safeguard confidentiality. Staff sensitive information relates to such matters as salary details, health information, disciplinary matters and any information relating to the member of staffs private life that the member of staff has not made public e.g home telephone number.

These items include:

Surname
Initials
Date of Birth
Postcode
Sex
National Insurance Number
Salary details
Forename
Address
Occupation
NHS or Staff number
Ethnic Group
Telephone number

What is Corporate information.

All items of information which relate to the running of the Trust. All such information should be regarded as confidential even if it maybe released under the Freedom of Information Act. This includes:-

Board Papers
Minutes of meetings
Details of contracts entered into
Financial information

1.3 Who is an authorised person?

An authorised person is anyone who needs to know the information to fulfil the responsibilities of their post. Do not assume that all of your work colleagues are authorised to see the same information that you are. If you are in doubt as to whether you should share the information with one of your colleagues, seek the advice of your manager in the first instance.

1.4 Inappropriate use of information systems

It is not acceptable for staff to access records on computer systems on behalf of themselves, relatives, friends or neighbours. There are proper channels for accessing this information. Do not access patient or staff information for anything other than your official duties, as misuse of the computer system may result in disciplinary action. Staff and patients have rights of access to their own records under the Data Protection Act 1998. The procedure for handling Access Requests to the Health Record details the process that should be adhered to.

1.5 What is meant by the transfer of patient identifiable information?

Examples of transferring personal identifiable information are:

- taking a document and giving it to a colleague
- making a telephone call
- Sending an email
- sending a fax
- passing information held on computer

In all cases, however simple or complicated, the principles of the Data Protection Act 1998 must be adhered to, in order to ensure that personal identifiable information is not disclosed inappropriately. Refer to Part Three 1.2

2.0 Physical Security

2.1 Room Access

Access should be restricted to any rooms containing identifiable information. Information should be kept securely within the locked environment when not in use

2.2 Safeguarding Information

Never leave personal identifiable information around for others to find

- Do not walk away from your work area leaving any documents exposed for unauthorised persons to see
- Only have the minimum information necessary on your desk for you to carry out your work. Any other related information should be put away securely
- Do not pass documents containing personal identifiable information to other colleagues by leaving it on a secretary’s desk or in an “in” tray. Always ensure that information is in a sealed envelope addressed to the recipient and clearly marked “Confidential”
- Wherever possible, avoid taking confidential information away from your work premises. Where this is necessary in order to carry out your duties (e.g. home

visits to a patient), you must keep the information securely locked away and make every effort to ensure that it does not get misplaced, lost or stolen. It is acknowledged that it is sometimes appropriate and necessary to leave notes with patients.

- When disposing of paper-based information, ensure that it is disposed of appropriately. Never put confidential information directly into a general waste paper bin or recycling bin
- Working diaries can hold a great deal of personal information and should be kept secure when not in use. Precautions should also be taken when transporting your diary to ensure it is in your care at all times. When you have finished with it or if you leave your job it should be handed in to your line manager who will ensure that it is retained for the appropriate length of time
- If information is no longer required, it should be disposed of appropriately. If information is required for an ongoing purpose, it should be locked securely away
- If documents containing personal identifiable information come into your possession and you are not the intended recipient, you should forward these to the intended recipient. If you identify any document containing personal information, such as letters or results, you should make every effort to decrease the possibility of these being seen by inappropriate persons.

Remember you are bound by the same rules of confidentiality whilst away from your place of work, as you are when you are at your desk. If you are working in a community setting it is understood that relevant information travels with you.

2.3 The physical transfer of information

When transferring paper notes, which contain personal identifiable information, make sure "Confidential" is marked in a prominent place on the front of the envelope. Ensure that the address of the recipient is correct and clearly stated, using the following format:

- Full name;
- Designation (job title);
- Department;
- Organisational address;
- Write a return address on the back of the envelope – giving only generic details or PO Box Number;
- Where possible patient notes should be hand delivered or collected;
- Do not use transit envelopes;
- Do not use patient labels.

Ensure arrangements are in place to check that notes have been safely received e.g. asking the recipient by phone or e-mail that they have received the confidential information.

Use the tracking system to ensure the movement of notes can be followed throughout their journey. Ask your line manager if you are unsure about this.

2.3.1 Transporting records by car

Records should never be left on view in a vehicle. Records must never be left in vehicles overnight.

2.3.2 Transporting records when on client visits

Ensure records are kept securely and not on view. Where several visits are involved, care must be taken to ensure only individual patient notes that are required are taken into that patient's home

2.3.3 Transporting records when on patient visits and not returning to base or starting visits from home

When it is not practicable to return notes to base after visits, confidentiality must be maintained within the home. Records must not be left in vehicles overnight and records should be returned to base as soon as is practicable.

2.3.4 Transporting Bulk Records

When transferring electronic and paper based records in bulk (in excess of 21 records), care must be taken to ensure this is done in a secure way. Secure external electronic transfer of data means information is sent between NHS.net accounts or, where data is transferred via another medium, using the AES 256bit encryption standard. Anyone not familiar with encryption must consult the NHS Information Security Policy or contact the Information Governance Team for guidance.

2.4 Transferring Paper or Electronic Personal Information by Courier

If a courier service is being used (to transfer paper or electronic confidential information), then it must be authorised by the Trust and must allow tracking of the package throughout its journey including recorded delivery. If this is not practicable then secure delivery via Royal Mail should be considered

- The proposed transfer must be approved by your Manager
- Any personal identifiable information which is to be transferred on portable electronic media must be encrypted to the recommended standard
- Always ensure that the recipient knows exactly when to expect the envelope/package
- Ask the recipient to contact you immediately they receive the package

2.5 Conversations

Ensure you cannot be overheard by unauthorised people when making sensitive telephone calls, during meetings, and when you are having informal discussions with colleagues about confidential information. Do not identify a patient or staff member by name unless it is safe to do so. If personal identifiers are necessary, please remember the following:-

- Consideration needs to be given to the position of any answerphone to ensure that recorded conversations cannot be overhead or otherwise inappropriately accessed;

- You must never leave any confidential data on any voicemail/telephone answering machine;

- When asking for a patient or member of the public to confirm their identity you must ask them to provide the following information but you must **never** provide them with the information to confirm
  Their name
  Their address
  Telephone number (if held)
  The name of their GP or practice they are registered with;

- Relatives, carers and friends regularly telephone asking for information relating to inpatients. It must not be assumed that the person in hospital wishes to be contacted by the caller. Staff should ask those telephoning to provide the following information before any information is disclosed
  The name of the person calling
  Name and address of the person they wish to contact
  Their relationship with the patient
  What ward the patient is on
  Why the patient is in hospital;

- The call should then be forwarded to the appropriate ward who should then ask the patient if they wish to speak to the caller;

- If the patient is asleep or unavailable the caller should be informed that the patient cannot be contacted at the present time;

- In clinical areas staff should be aware that other patients in the same room/ward might overhear them. Whilst it is appreciated that it is difficult to manage confidentiality in situations like these, staff are expected to be aware of the possible problems and do all they can to respect the patients' right to confidentiality;

- It is not appropriate to discuss personal information in public areas eg corridors, stairways, shuttle bus, occupied lifts or staff canteen;

- When speaking to a patient, carer or staff member on the telephone, confirm the caller's identity and ensure they are entitled to the information they are requesting. If in any doubt about the identity of the caller take their telephone number, verify it independently and call them back via the switchboard;

- Be aware of bogus callers. These can be lone individuals, private investigators or individuals working for debt collection agencies who have been sub-contracted. Extreme vigilance is required at all times. Always verify a caller's details and ensure they are entitled to the information they are requesting before you release it. Alert your line manager if you suspect an instance of a bogus caller;

- Patient information may be released in cases where there is a danger to patients or others. This decision should always be made by the patient's clinician or other designated senior person. Even in these cases you should limit the transfer to specific and relevant items only, do not release everything in the record. Always document the justification for releasing the information;

- Identifiable information should not be used in training, testing systems, or demonstrations without explicit consent. Test data should be used for this purpose;

- If you have to leave the phone unattended ensure the hold/mute button on your telephone is activated;

- If in doubt, always ask. Consult your line manager in the first instance or contact the Information Governance Team on 0845 1272600.

2.6 Sending personal information by fax

This should only happen when all other alternatives have been considered you must anonymise confidential information whenever you can.
When sending faxes that contain personal identifiable information you must use a designated Safe Haven fax wherever possible. A designated Safe Haven is a place where a fax containing confidential information can be sent safely in the knowledge that procedures are in place at the other end to ensure its security. If you cannot access a designated Safe Haven fax machine the following principles must be followed:

- Always use a fax cover sheet, complete with the senders and recipients details and the number of pages to be faxed;
- Telephone first to inform the recipient that you are faxing confidential information;
- Ask if they could wait by their fax machine whilst you send the fax;
- Ask if they could telephone to acknowledge receipt or contact them immediately after sending to confirm they have received all sent pages;
- Always double check that you have keyed in the right number before hitting the “send” key;
- Regularly used numbers should be programmed into your fax machine (if possible) to decrease the possibility of keying in the wrong number;
- If you have not sent information to a particular fax number before send a test fax to ensure it is the correct number;
- Remove documents immediately from the fax machine once they have been sent;
- Do not leave the fax machine unattended whilst faxing confidential information;
- If the fax is not collected immediately by the recipient it should be placed in a sealed envelope with their name and ‘confidential’ written on it;
- If you find confidential information left on a fax machine return it in a sealed envelope to the sender. If the sender is unknown, shred the fax;
- Never send faxes to destinations where you know they are not going to be seen for some time or outside office opening hours;
- Display a poster next to the fax machine to remind users of the above points;
- It is advisable to have an audit trail of what has been faxed, by whom and to what location.

2.7 Keeping Computerised Information Safe

The security and confidentiality of information held on computer must be maintained at all times.

- Never leave a computer logged on to a system and unprotected. Always protect the system by pressing Control, Alt & Delete simultaneously on your keyboard and select the option ‘lock computer’. This applies no matter how long you are leaving your computer unattended;
- Always log off when you have finished. This prevents the risk of unauthorised access to patient information. It also ends the users session on the computer. Turn off the computer at the end of the working day. If it is necessary to leave it switched on for technical reasons make sure it is locked using Control, Alt & Delete plus option ‘lock computer’;
- Where it is necessary for personal identifiable information to be stored ensure that it is stored in a secure way with password protection;
- Never store personal identifiable information on the hard disk of the computer (either on the c-drive, desktop or ‘my documents’). Seek guidance from the Information Governance Team on x5000;
- Documents or files stored on the network must not be subject to separate password protection. If access to files or folders needs to be restricted this can be arranged via the Service Desk;
- Do not keep any personal identifiable information longer than necessary;
- Delete files you do not need to keep and if the information is stored on removable media ensure that it is clearly labelled and locked away. When the information held is no longer required the removable media eg encrypted memory stick must be reformatted, erased or destroyed in accordance with the Trust’s Healthcare Records Management Policy;
- Windows users should remember that when deleting files they are moved to the “recycle bin”. Therefore, the recycle bin should be emptied on a regular basis. If in doubt, check with the IT Service Desk;
- Passwords protect both the information and you as a user. Never disclose your password to anyone under any circumstances. Never write your password down and always change your password when prompted. It is recommended that passwords should be a minimum of 8 characters and be a mixture of letters and numbers ;
- Never use anyone else’s password, login or PIN number. Never, as a manager, ask anyone to use another’s password for convenience. If it is absolutely necessary contact the IT Service Desk;
- If you are issued with a Smartcard you must keep it secure and not permit anybody else to use it. You must not share your PIN or password with any other user. If you lose your Smartcard or suspect it has been stolen or used by a third party you must report the incident to your local Registration Authority as soon as possible via your line manager;
- Destruction and/or disposal of computers, or parts thereof, must be carried out by the IT Department. Contact the IT Service Desk for assistance on 0845 1272600;
- **Staff must not store any personal or sensitive personal information on any type of privately owned computer or storage device unless this action has been approved by the Trusts SIRO;**
- Identifiable information should not be used in training, testing systems or demonstrations. Test data should be used for these purposes.

2.7.1 Safeguarding Information when sending out of the European Economic Area (EEA)

Principle 8 of the Data Protection Act places extra requirements on your organisation for any transfers of personal information outside of the EEA.
If any information is to be transferred, stored or processed outside of the EEA contractual arrangements must be in place. The contract must clearly state that the information will meet the same standards of Data Protection as if it was stored or processed within the EEA.
If any member of staff is intending to transfer personal information outside the EEA they must obtain advice from the Caldicott Guardian or Information Governance Team.

2.7.2 If you use a portable device

Portable devices include laptop computers, iPads, smart phones (iPhone, blackberry etc), DVD's and memory sticks

- All staff must adhere to the following when using any portable device;
- All portable equipment must be encrypted;
- Laptops that have identifiable information stored on them **must not** be taken off NHS premises unless the information is encrypted;
- Do not leave portable computer equipment on view within your car;
- Do not leave portable computer equipment in your car overnight;
- Store any back-ups (DVD's, memory sticks, etc) securely. Update your information regularly whilst using portable equipment;
- Ensure that your computer is password protected;
- Ensure that any document, spreadsheets or databases containing confidential or sensitive data are password protected;
- All equipment should be secure when not in use;
- Make every effort to ensure that your portable device does not get misplaced, lost or stolen.

Remember, you are bound by the same rules of confidentiality whilst away from your place of work, as you are when you are at your desk.

2.7.3 Use of removable data storage devices

- Removable data storage devices (USB sticks, data sticks, USB flash drives, etc) should only be used to transport or store data when other more secure means, such as network shared folders are not available and your Line Manager or the Trusts SIRO has approved this action;
- Ask the IT Service Desk for advice as to the most appropriate and secure method;
- All removable data storage devices must be encrypted and stored in a secure environment;
- Ensure that data is only held on the removable data storage device for a specific purpose and has been approved by your Line Manager or SIRO;
- As soon as is practicable move the data file(s) back on the secure network and delete from your device.

2.8 Use of the e-mail system (The email policy is available on the intranet)

You are responsible for the contents of your e-mails

- You must not disclose your login to anyone
- Remember to log out of the system when you are leaving your computer unattended or lock your computer using the Control/Alt & Delete keys together and selecting 'lock computer' option
- Confidential data may only be transmitted via email as set out in the Trusts email Policy
- Identifiable information that is received in an e-mail from outside the NHS should be dealt with quickly and safely. Save the information to a suitable folder on the network and delete the file from your inbox
- Ensure that the content of email is not sexually or racially offensive, or otherwise illegal in nature
- Archive emails to the network not to the hard drive of the computer. Ask the IT Service Desk if unsure

For further information see the Trusts E-mail Use Policy

2.9 Text Messaging

Short Message Service (SMS) is an easy to use, standardised, mobile communications service for the exchange of short alphanumeric text messages, usually between mobile telephone devices.

SMS or text messaging is an attractive technology for quick communication of short messages and is a widely accepted form of communication. Patients therefore increasingly expect organisations to communicate with them in this way for simple transactions such as appointment reminders.

The Trust endorses the use of SMS to communicate with patients provided this is for simple communications such as appointment reminders, and provided strict organisational protocols (outlined below) are followed when sending messages:

- Only Trust approved systems may be used when sending out appointments or reminders. This means that teams / services must either set up a generic (team account) or individual nhs.net email account prior to sending SMS messages to patients;
- SMS messaging must not be used for sensitive personal information such as test results or discharge summaries. It must be used only for appointments and other non-sensitive information;
- Under NO circumstances whatsoever should any type of confidential data be transmitted via SMS.

3. Record keeping best practice

The Health Care Records Management Policy has been produced to ensure that the organisation can control both the quality and quantity of the information that it generates

The Health Care Records Management Policy relates to information in any medium e.g. paper, microfiche, microfilm, audio tapes, video tapes, X-ray images, databases, notes, e-mail etc, which has been gathered as a result of any NHS activity whether clinical or non clinical by employees – including external consultants, agency or casual staff.

3.1 White Boards

White Boards or name boards above patient beds and in other areas should only state the patients name (preferably initials). If the patient insists that they do not want their information displayed you must respect their wishes.

No other patient identifiable information should be put onto White Boards in public areas for example address, date of birth.

3.2 Pseudonymisation

It is NHS policy and a legal requirement that when patient information is used for purposes not involving the direct care of the patient (i.e. secondary use) the patient should not be identified. Examples of secondary uses include commissioning, payment by results (PbR), performance management, capacity planning, service redesign and benchmarking.

Pseudonymisation is a method which disguises the identity of patients by creating a pseudonym for each patient identifiable data item.

Patient identifiable data intended to be used for secondary uses must ideally be sourced from the Trusts Information Teams, who will de-identify the data appropriately before the data is passed on to the intended recipient to be used for secondary purposes.

If any member of staff needs to use patient identifiable information for secondary use then they must seek advice and guidance from their manager.

4. Training & Implementation

All staff will be made aware of their responsibilities for confidentiality through generic and specific training programmes and guidance.

All employees of the Trust must comply with the minimum training requirements set out below:

- Information Governance element of Trust Induction Programme;
- Information Governance e-learning module;
- Risk Management Mandatory Training (Information Governance element).

Part Three - Legal Considerations and Guidance

1 Legal Considerations

There are a range of statutory provisions that limit or prohibit the use and disclosure of information in specific circumstances and, similarly, a range of statutory provisions that require information to be used or disclosed. Legal requirements and permissions are continually being added to, if you require further information please contact the Information Governance helpdesk.

Generally, however, there are four main areas of law, which constrain the use and disclosure of personal information. These are briefly described below.

1.1 Common Law Duty of Confidentiality

This is not codified in an Act of Parliament but built up from case law where practice has been established by individual judgments. The key principle is that where consent has been obtained information should not be used or disclosed further, except as originally understood by the consenter, or with their subsequent consent. Whilst judgements have established that confidentiality can be breached 'in the public interest', these have centred on case-by-case consideration of exceptional circumstances. Confidentiality can also be overridden or set aside by legislation.

"All NHS bodies and those carrying out functions on behalf of the NHS have a common law duty to support professional ethical standards of confidentiality. Everyone working for or with the NHS who records, handles, stores or otherwise comes across information that is capable of identifying an individual patient, has a personal common law duty of confidence to patients and to his or her employer". (The Protection and Use of Patient Information: Guidance from the Department of Health HSG (96)18)

This statement applies equally to employed staff, students, voluntary staff and trainees on placements.

1.2 Data Protection Act 1998 (DPA98)

This Act provides a framework that governs the processing of information that identifies living individuals and contains personal data[2]. Processing includes holding, obtaining, recording, using and disclosing of information and the Act applies to all forms of media, including paper and images.
The DPA98 imposes constraints on the processing of personal information in relation to living individuals. It identifies eight data protection principles that set out standards for information handling.

- the 1st, requires processing to be fair and lawful and imposes other restrictions;

[2] **Patient Information** Personal data is defined under the DPA98 as 'data which relate to a living individual who can be identified – (a) from those data, or (b)from those data and other information which is in the possession of, or likely to be in the possession of, the data controller – and includes any expression of opinion about the individual and any indications of the intentions of the data controller or any other person in respect of the individual'.

- the 2nd, requires personal data to be processed for one or more specified and lawful purposes;
- the 3rd, requires personal data to be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed;
- the 4th, requires that data shall be accurate and, where necessary, kept up to date;
- the 5th, requires personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose(s);
- the 6th, requires that personal data shall be processed in accordance with the rights of the data subjects under the Act;
- the 7th, requires personal data to be protected against unauthorised or unlawful processing and against accidental loss, destruction or damage; and
- the 8th, which requires that personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data.

1.3 Human Rights Act 1998 (HRA98)

Article 8 of the HRA98 establishes a right to 'respect for private and family life'. This reinforces the duty to protect the privacy of individuals and preserve the confidentiality of their health records. Current understanding is that compliance with the Data Protection Act 1998 and the common law of confidentiality should satisfy Human Rights requirements.

Legislation generally must also be compatible with HRA98, so any proposal for setting aside obligations of confidentiality through legislation must:

- pursue a legitimate aim;
- be considered necessary in a democratic society; and
- be proportionate to the need.

There is also a more general requirement that actions that interfere with the right to respect for private and family life (e.g. disclosing confidential information) must also be justified as being necessary to support legitimate aims and be proportionate to the need

1.4 Administrative Law

Administrative law governs the actions of public authorities. According to well-established rules a public authority must possess the power to carry out what it intends to do. If not, its action is *"ultra vires"*, i.e. beyond its lawful powers. It is also necessary that the power be exercised for the purpose for which it was created or be "reasonably incidental" to the defined purpose. It is important that all NHS bodies be aware of the extent and limitations of their powers and act *"intra vires"*.

The approach often adopted by Government to address situations where a disclosure of information is prevented by lack of function (the ultra vires rule), is to create, through legislation, new statutory gateways that provide public sector bodies with the appropriate information disclosure function. However, unless such legislation explicitly requires that confidential patient information be disclosed, or provides for common law confidentiality obligations to be set aside, then these obligations must be satisfied prior to information disclosure and use taking place, e.g. by obtaining explicit patient consent.

2 Department of Health Requirements

In addition to the obligations of law, the Department of Health and the professional bodies require that all staff working for the health service comply with the principles set down by the Caldicott Report, Caldicott 2 and the NHS Confidentiality Code of Practice.

2.1 Caldicott Report

The Caldicott Committee, Chaired by Dame Fiona Caldicott, was set up by the Chief Medical Officer for Health following increasing concerns regarding the way information flowed, not only within NHS organisations, but to and from non-NHS organisations also. The resulting report, "The Caldicott Committee: Report on the Review of Patient Identifiable Information" was published in December 1997.

The Report made sixteen recommendations. One of the recommendations was the appointment of a Caldicott Guardian, who should be a senior health professional or an existing member of the management board, for each organisation. The Guardian is responsible for agreeing and reviewing protocols for governing the disclosure of personal identifiable information across organisational boundaries.

The Committee also developed a set of 6 general principles for the safe handling of personal identifiable information and these Principles are the guidelines to which the NHS works. They work hand-in-hand with the Principles of the Data Protection Act 1998. They both cover information held in whatever format – electronic, paper, verbal or visual. The seven Caldicott Principles must be adhered to when collecting, transferring or generally working with personal identifiable information.

The Caldicott Principles -

i. Justify the purpose for using confidential information
ii. Don't use patient identifiable information unless it is absolutely necessary
iii. Use the minimum necessary patient identifiable information
iv. Access to patient identifiable information should be on a strict need to know basis
v. Everyone should be aware of their responsibilities
vi. Understand and comply with the law
viii. The duty to share personal confidential data can be as important as the duty to respect service user confidentiality

2.2 The NHS Confidentiality Code of Practice

The NHS Confidentiality Code of Practice was published by the Department of Health in November 2003 following a major public consultation. The consultation included patients, carers and citizens, the NHS, other health care providers, professional bodies and regulators.

The NHS Confidentiality Code of Practice is a guide to required practice for those who work within or under contract to NHS organisations. It replaces previous guidance, HSG (96)18/LASSL (96)5 – The Protection and Use of Patient Information and is a key component of emerging information governance arrangements for the NHS.

Each Organisation has a mandatory obligation under the Information Governance Toolkit to produce a local confidentiality policy.

Appendix A

References and Further reading:

DoH Confidentiality - NHS Code of Practice
Copies can be downloaded from the Department of Health website: www.dh.gov.uk

GMC – Confidentiality : Protecting and Providing Information
Accessed via the General Medical Council website: www.gmc-uk.org

BMA – Confidentiality & Disclosure of Health Information
Accessed via the British Medical Association website: www.bma.org.uk

Confidentiality: What You Need To Know Booklet - Copies can be obtained from theTrusts Intranet

NHS Information Governance : Information Security Policy
Copies can be downloaded from the Connecting for Health website: www.connecting for health.nhs.uk

Contact Details:

Information Governance Service – X5000

IT Service Desk – ext 5000, option 4 or switchboard DDH for external calls 01924 512000

EQUALITY IMPACT ASSESSMENT FORM

INITIAL ASSESSMENT/SCREENING

An impact assessment is a way of finding out whether an existing or proposed policy affects different groups of people in different ways and whether there is adverse impact on a group.

Managers Name **Heather Cook**	**Directorate** **Corporate**
Policy Title **Confidentiality Policy Statement and Supporting Guidance**	
Policy Statement This Policy statement applies to all personal identifiable information, whether written, computerised, visual, audio or held in the memory of a member of staff. It applies equally to staff on permanent, temporary or voluntary contracts. Health care professionals and the staff that support them hold information about people that may be private and sensitive. Patient information is collected to provide care and treatment to individuals and generally must not be used for other purposes without their consent. In the same way, information about staff that is processed for the purpose of their employment is confidential. Confidentiality should only be breached in exceptional circumstances and with appropriate justification and be fully documented.	
Which groups does the policy benefit **All**	
Related polices that may be affected by changes This Policy cross references several other policies ie, Network Security Policy, Internet Use Policy, Email policy, Information Security Policy etc.	
Names of staff and public (if applicable) who participated in the assessment, date of assessment **None** **Indicate either Y or N in each Box below in answer to the following questions/statements (cannot be both Y & N in same box or left blank)**	

	Age	Disability	Ethnicity	Religion and belief	Gender/ transgender	Sexual Orientation
Do different groups have different needs, experiences, issues and priorities in relation to the policy or service?	**N**	**N**	**N**	**N**	**N**	**N**
Is there potential for or evidence that, the policy or service will discriminate against certain groups?	**N**	**N**	**N**	**N**	**N**	**N**
Is there public concern in the policy area about actual, received or potential discrimination against particular groups?	**N**	**N**	**N**	**N**	**N**	**N**
Is there doubt about answers to any of the above questions	**N**	**N**	**N**	**N**	**N**	**N**

This form is to be used for new and existing policies and service developments, where a question is not applicable to your assessment, please indicate.

If the answer to any of the above is ‘yes’ an Intermediate assessment in the relevant area(s) is required. If not please complete below and then submitted to the relevant board/committee for approval.

Following completion of the above assessment please state the names of the staff/Director and then please identify the correct EQIA statement and delete the others.

Names of Staff/Public undertaking assessment: **Date: November 2016**

Director’s name: Heather Cook