



*Yorkshire and the Humber*

# **CONFIDENTIALITY POLICY STATEMENT AND GUIDANCE**

**Updated: November 2009**

## CONTENTS

Section	Description	Page
<b>CONFIDENTIALITY POLICY STATEMENT</b>		
<b>1</b>	Purpose	<b>5</b>
<b>2</b>	Supporting Guidance	<b>6</b>
<b>3</b>	The Policy Statement	<b>6</b>
<b>4</b>	Contract of Employment	<b>7</b>
<b>CONFIDENTIALITY POLICY STATEMENT – GUIDANCE</b>		
	Summary	<b>8</b>
<b>Part One</b>	<b>Confidentiality</b>	
<b>1</b>	Statement of Confidentiality	<b>9</b>
<b>2</b>	Duty of Confidence	<b>10</b>
<b>3</b>	Using and disclosing confidential patient or person identifiable information	<b>10</b>
<b>4</b>	Patient Data and Smartcards	<b>11</b>
<b>5</b>	Protecting Information	<b>11</b>
<b>Part Two</b>	<b>Confidentiality : The Practical Application</b>	
<b>1</b>	Definitions <ul style="list-style-type: none"> <li>• What is patient indefinable information? <span style="float: right;"><b>12</b></span></li> <li>• What is staff identifiable information? <span style="float: right;"><b>12</b></span></li> <li>• Who is an authorised person? <span style="float: right;"><b>12</b></span></li> <li>• Inappropriate use of information systems <span style="float: right;"><b>13</b></span></li> <li>• What is meant by the transfer of person identifiable information? <span style="float: right;"><b>13</b></span></li> </ul>	
<b>2</b>	Physical Security <ul style="list-style-type: none"> <li>• Room Access <span style="float: right;"><b>13</b></span></li> <li>• Safeguarding Information <span style="float: right;"><b>13</b></span></li> <li>• The physical transfer of personal information <span style="float: right;"><b>14</b></span></li> <li>• Transporting records by car <span style="float: right;"><b>14</b></span></li> <li>• Transporting bulk records <span style="float: right;"><b>15</b></span></li> </ul>	

<b>Section</b>	<b>Description</b>	<b>Page</b>
	<ul style="list-style-type: none"> <li>• Conversations <b>15</b></li> <li>• Sending personal information my fax <b>16</b></li> <li>• Safeguarding computerised information <b>16</b></li> <li>• Safeguarding information when sending out of the European Economic Area (EAA) <b>18</b></li> <li>• If you use a portable computer outside your place of work <b>18</b></li> <li>• Use of removable data storage devices <b>18</b></li> <li>• Use of the e-mail system <b>19</b></li> </ul>	
<b>3</b>	Record keeping best practice	<b>19</b>
<b>4</b>	Breaches of Confidentiality	<b>20</b>
<b>5</b>	Termination of employment or contract with the SHA	<b>20</b>
<b>Part Three</b>	<b>Legal considerations and guidance</b>	
<b>1</b>	Legal Considerations <ul style="list-style-type: none"> <li>• Common Law Duty of Confidentiality <b>21</b></li> <li>• Data Protection Act 1998 (DPA 98) <b>22</b></li> <li>• Human Rights Act 1998 (HRA 98) <b>22</b></li> <li>• Administrative Law <b>23</b></li> </ul>	
<b>2</b>	Department of Health requirements <ul style="list-style-type: none"> <li>• Caldicott Report (including The Caldicott Principles) <b>23</b></li> <li>• The NHS Confidentiality Code of Practice <b>24</b></li> </ul>	
<b>Appendix A</b>	References and further reading	<b>25</b>
<b>Appendix B</b>	Confidentiality Declaration	<b>26</b>

## POLICY REFERENCE INFORMATION

Policy Reference	Confidentiality Statement and Guidance
Version Number	2.0
Status	Final
Author	Richard Powell Corporate Business Manager
Lead Director	Director of Finance and Investment (SIRO)
Implementation Date	November 2009
Date of Last Review	June 2008
Date of Next Review	November 2010

## DOCUMENT REVISION RECORD

Version	Description of Changes	Reason for Change	Author	Date
1.0	-	-	-	-
2.0	Various	➤ To incorporate and take account of issues around commercial confidentiality	Richard Powell	October 2009

# YORKSHIRE AND THE HUMBER STRATEGIC HEALTH AUTHORITY

## CONFIDENTIALITY POLICY STATEMENT

### 1. Purpose

The principal objective of this Policy Statement is to ensure that all staff within Yorkshire and the Humber Strategic Health Authority (the SHA) and organisations and programmes hosted by the SHA are aware of their responsibilities with regards to confidential information. **For the purposes of this document, the term 'SHA' referred to throughout means the Strategic Health Authority and the organisations and programmes which are hosted by the Strategic Health Authority.**

As a public body the SHA has a statutory duty to safeguard the Confidential Information it holds, from whatever source, that is not in the public domain.

This policy applies to any individual, company or firm working within or for the SHA. Without limitation, this includes all employees of the Department of Health and NHS Business Services Authority, workers, individuals on fixed term contracts, interim resource, secondees, volunteers, temporary and permanent contractors, agency workers, temporary administrative resource and/or any other third party service providers.

The principle underpinning this policy statement is that no individual or company working for or with the SHA 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
- Freedom of Information Act 2000
- Public Interest Disclosure Act 1998
- Human Rights Act 1998
- The Computer Misuse Act 1990
- Common Law Duty of Confidentiality
- The Caldicott Report 1997
- The NHS Confidentiality Code of Conduct

The following SHA Policies should also be referred to:

- E-mail Policy
- Internet Policy
- Records Management Policy and Retention Schedule
- Registration Authority (RA) Procedures Document

All departments within the SHA should establish working practices that effectively deliver the level of confidentiality that is required by law, ethics and this policy statement. The practices should be continually reviewed.

## **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 appended guidance.

Staff working for or within the SHA should familiarise themselves with their obligations in relation to confidentiality and IM&T security on their first working day and routinely via mandatory e-learning training packages. This is supported by literature and the Confidentiality & IM&T Helpdesk service which can be contacted on **0845 1272600**

## **3. The Policy Statement**

**During the course of their day to work, many individuals working within or for the SHA will often handle or be exposed to information which is deemed personal, sensitive or confidential, which may include commercial confidential information.**

**It is a requirement that any individual, company and firm to which this Policy applies shall not at any time during the period they work for or provide services to the SHA nor at any time after its termination, disclose confidential Information that is held or processed by the SHA.**

**Confidentiality should only be breached in exceptional circumstances and with appropriate justification and be fully documented.**

**All staff should ensure that the following principles are adhered to:-**

- **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 or disposed of;**
- **Access to confidential information should be on a need-to-know basis**
- **Every effort should be made to inform individuals how their information is going to be used and who it will be shared with and why it may be shared**
- **When an individual consents 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 an individual withholds consent, or if consent cannot be obtained, disclosures may be made only where:**
  - a. **They can be justified in the public interest (usually where disclosure is essential to protect someone from the risk of significant harm)**

- b. They are required by law or by a court order**
- **Only as much information that 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.**
- **Any doubts at all about disclosure must be discussed with either your line manager or the Confidentiality and IM&T Security Helpdesk.**

#### **4. Contract of Employment**

The majority of contracts of employment include 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.

# YORKSHIRE AND THE HUMBER STRATEGIC HEALTH AUTHORITY

## CONFIDENTIALITY POLICY STATEMENT: GUIDANCE

### 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 information and commercial confidential information. 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 three.

The guidance should ensure 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.

It is compulsory that all individuals working for the SHA or those staff from other organisations undertaking work on behalf of the SHA should personally read, accept and sign the Confidentiality Policy prior to commencing work on his or her first day. The Confidentiality Policy must be understood and the declaration at the back of this policy accepted and/or signed prior to accessing any systems or documentation.

It is compulsory that all existing individuals working for and/or within and/or providing services to the SHA understand and accept this Policy. Any future amendments to the policy will require all individuals working within / for the SHA to accept the revised version.

The objective of the policy is that of continuously enforcing the need for confidentiality.

- 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 have 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 the person who has provided the information and the recipient of the information. Without that level of trust, the person who has provided the information may be reluctant to impart the necessary information for whatever purpose it is required. In this policy statement “person” includes an individual, partnership, firm, trust, body corporate, government, government body, authority, agency, unincorporated body of persons or association and any reference to a “person” includes reference to that person’s successors and permitted assigns.
- 1.2 Confidential and sensitive information utilised by the SHA can be taken in many different forms. In addition to confidential and sensitive information arising in the course of the SHAs general day to day work, due consideration should also be given to the following which without limitation may constitute commercial confidential information:
- Ideas/programme plans/forecasts/risks/issues
  - Trade secrets
  - Business methods and business design
  - Finance/budget planning/business cases
  - Prices and pricing structures
  - Sources of supply and costs of equipment and/or software
  - Prospective business opportunities in general
  - Computer programs and/or software adapted or used
  - Policy advice and strategy
  - Corporate or personnel information
  - Contractual and confidential supplier information
  - Patient and GP data and that of associated Health Organisations
  - Any information designated commercial in confidence
- 1.3 Confidentiality should only be breached in exceptional circumstances and with appropriate justification. When a health care professional can justify that information should be released they should act promptly to disclose all relevant information. This is often essential in 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. Any breach of staff information must be fully documented giving justification for the breach.

## **2. Duty of Confidence**

2.1 A duty of confidence arises when one person discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence. The obligation to maintain, preserve and respect confidentiality is:

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

2.2 An individual shall not be restrained from using or disclosing any Confidential Information where:

- that individual has been duly authorised to do so by the person or persons who have a right of confidentiality in respect of the Confidential Information; and/or
- the Confidential Information has entered the public domain unless it enters the public domain as a result of an unauthorised disclosure by the individual; and/or
- the Confidential Information has entered the public domain by an authorised disclosure for an authorised purpose; and/or
- the Confidential Information is required to be disclosed by law; and/or
- disclosure is permitted under the Public Interest Disclosure Act 1998 provided that any such disclosure is made in an appropriate way to an appropriate person having regard to the provisions of that Act.

2.3 All individuals must exercise all due care and diligence to prevent unauthorised disclosure of Confidential Information.

2.4 Information that can identify individuals must not be used or disclosed for purposes other than that for which it was collected without the individual's explicit consent, some other legal basis, or where there is a robust public interest or legal justification to do so. It should be noted that information about an individual, without a name or identifier, may still contain sufficient information to identify the person, in which case it must be treated as confidential.

## **3. Using and disclosing confidential patient or person identifiable information**

3.1 Should staff encounter information relating to individuals then it should be processed in the manner outlined below.

3.2 Individuals should be informed about

- The use and disclosure of the information associated with their information; and

- The choices that they have and the implications of choosing to limit how information may be used or shared;

#### **4. Patient Data and Smartcards**

- 4.1 Access to certain elements of patient and person identifiable data is only possible with a Smartcard which can be obtained from a Registration Authority Manager or Agent at the local Registration Authority located within the employing organisation.

#### **5. Protecting information**

- 5.1 It is essential that personal, confidential and commercially sensitive information is effectively protected against improper disclosure at all times.

- 5.2 Many improper disclosures are unintentional

- Specific cases should never be discussed where it is possible that you could be overheard;
- Records relating to individuals, for example staff members, either on paper or on screen, should not be left where they can be seen by any unauthorised person;
- All Personal Information must be stored securely;
- All commercial confidential information must be stored securely.

## **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	Forename
Initials	Address
Date of Birth	Other dates (e.g., death, diagnosis)
Postcode	Occupation
Sex	NHS number
National Insurance Number	Ethnic Group

Local Identifier (e.g., hospital or GP Practice Number)  
Telephone Number

#### **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.

These items include:

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

#### **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. Further information can be obtained from the Corporate Business Team on (0113) 295 2051.

## 1.5 **What is meant by the transfer of person identifiable information?**

Examples of transferring personal identifiable information are:

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

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. **Physical Security**

### 2.1 **Room Access**

Access should be restricted to any rooms containing identifiable and commercial confidence information. Information should be kept securely within the locked environment when not in use. Facilities such as lockable filing cabinets or desk drawers should be used wherever possible.

### 2.2 **Safeguarding Information**

- Never leave personal identifiable, confidential or commercially sensitive information around for others to find. Documents should be secured away when not in use.
- 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 the desk of a colleague 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 you must keep the information securely locked away and make every effort to ensure that it does not get misplaced, lost or stolen.
- When disposing of paper-based information, ensure that it is disposed of appropriately. Never put confidential information directly into a general waste paper recycling bin. Always use the dedicated confidential waste disposal units.
- If information is no longer required, it should be disposed of appropriately, in line with the SHA retention policy. 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, you should make every effort to decrease the possibility of these being seen by inappropriate persons. Such incidents should be reported using the SHA incident reporting procedures

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. For example, if you are working remotely from home or otherwise away from the office.

## 2.3 The physical transfer of personal information

When transferring records, 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 or staff records should be hand delivered or collected
- Do not use transit envelopes

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

### 2.3.1 Transporting records by car

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

### 2.3.2 Transporting Bulk Records

When transferring records in bulk (more than 51 records), care must be taken to ensure this is done in a secure way. Secure external transfer means information is sent between NHS.net accounts or, where data is transferred via another medium, using encryption software and encrypted devices approved by the SHA. Anyone not familiar with encryption technologies should contact the Confidentiality & IM&T Security Team for guidance by calling **0845 1272600**

### 2.4 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 answer phone to ensure that recorded conversations cannot be overheard or otherwise inappropriately accessed
- It is not appropriate to discuss personal information in public areas e.g. corridors, stairways or occupied lifts
- When speaking to a person on the telephone, whose identity you are unsure of, 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.
- 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 whilst on a call 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 Confidentiality & IM&T Security helpdesk

## 2.5 Sending personal information by fax

Do not routinely send identifiable information by fax. Justify the need to fax the information and anonymise confidential information whenever you can.

When sending faxes that contain personal identifiable information, try to use a designated Safe Haven fax number 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 should be followed:

- Always use a fax cover sheet, complete with the senders and recipients details
- 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 after sending
- 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
- Remove documents immediately from the fax machine once they have been sent
- Do not leave the fax machine unattended whilst faxing confidential information
- If a 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

## 2.6 Safeguarding Computerised Information

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

- All PCs must be password protected.
- 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

- All laptop computers or portable computer equipment should have their internal hard drives encrypted to the agreed SHA standard - AES 256. All portable computer equipment should be locked away when not in use, and NOT left unattended, or on desks overnight.
- Never leave a computer logged onto 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 confidential or personal information. It also ends the user's 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 saved, you should ensure that it is stored in a secure way with password protection. Consideration could be given to restrict access folders if required
- Never store personal identifiable information on the hard disk of the computer (either on the c-drive or 'my documents'). Seek guidance from the Confidentiality & IM&T Security Helpdesk
- Do not keep any personal identifiable information longer than necessary
- Delete files you do not need to keep.
- If information is stored on removable media ensure that it is clearly labelled and locked away. When information held is no longer required the removable media e.g. CD or DVD must be reformatted, erased or destroyed in accordance with the SHA's Records Management Policy and Retention Schedule. Contact one of the Facilities Managers or the IT Service Desk if you need advice.
- 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
- 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. Staff should familiarise themselves with both local and national guidance regarding proper use of Smartcards.
- Destruction and/or disposal of computers, or parts thereof, must be carried out by the IM&T Department. Contact the IT Service Desk for assistance
- Staff must never store personal identifiable information on a privately owned laptop or other portable device.

### 2.6.1 **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 Confidentiality & IM&T Security Team by calling **0845 1272600**

### 2.6.2 **If you use a portable computer / portable device provided by your workplace outside your place of work, the following must be followed:**

- All portable devices must be encrypted to agreed SHA standards.
- When travelling by car, all portable devices should be stowed away and transported in a locked boot and only left unattended for short periods. Do not leave portable computer / device or equipment on view within your car at any time.
- Do not leave portable computer / device equipment in your car overnight
- Store any back-ups (CDs, floppy disks, flash drives, etc) securely. Update your information regularly whilst using portable equipment
- Ensure that your computer / device is password protected
- Ensure that any document, spreadsheets or databases containing confidential or sensitive data are password protected. Staff should seek advice regarding password protection from the Service desk by calling **0845 1272600**
- All equipment should be locked away when not in use, staff using portable computer equipment / devices off site, are responsible for the safeguarding of the equipment.
- Make every effort to ensure that your portable computer / device does not get misplaced, lost or stolen
- Only copies of the data should be held on a portable computer. Original versions must be held on central network servers

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

### 2.6.3 **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.
- Ask the IT Service Desk for advice as to the most appropriate and secure method

- All removable data storage devices provided by your workforce should be stored in a secure environment and must be encrypted
- If an SHA member of staff needs to store any data on such a device, it must be a device provided by the SHA
- If an external agency needs to store any data on such a device, it must be specified by the SHA
- Ensure that data is only held on the removable data storage device for a specific purpose
  - As soon as is practicable move the data file(s) back on the secure network
  - Ensure that you keep a back up copy of all data files stored on your removable data storage device
- If person identifiable information or commercial confidential information is to be stored on any removable media then it must be encrypted to agreed SHA standards
- Only copies of the data should be held on removable media. Original versions must be held on central network servers

## 2.7 Use of the e-mail system

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
- Patient identifiable and sensitive staff identifiable information must **NOT** be sent in e-mails, unless special arrangements have been agreed in conjunction with the Caldicott Guardian or Senior Information Risk Officer (SIRO). Such information should be sent as a password protected attachment accompanying the e-mail with the password sent separately.
- 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 – see 2.6) 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 e-mails should be saved to the network and not to the hard drive of your computer. Exceptional cases should be considered on an individual basis and agreed with your Director.

For further information see the E-mail Use Policy

## 3. Record keeping best practice

The 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 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

#### **4. Breaches of Confidentiality**

It is important for the SHA to protect its legitimate business interests and in particular its Confidential Information, and that belonging to other persons and disclosed to the SHA in confidence. Breaches of confidentiality, of any sort, including breach of this Policy, will be regarded as serious misconduct and may result in:

- Dismissal
- Termination of secondment for secondees and a request for their employer to apply their internal disciplinary procedures
- Termination of contracts for interim resources, temporary workers, agency workers and/or contractors
- Legal action being taken against the discloser and/or any other third party

If an individual unintentionally divulges Confidential Information, or they are aware of any individual doing so, he or she must report it immediately to their line manager and/or to the HR Department

#### **5. Termination of employment or contract with the SHA**

On leaving or terminating a contract with the SHA, individuals should ensure that they return all equipment, including removable data storage devices, to their line manager. Individuals should also not retain files or information relating to SHA business including, but not limited to, documents, correspondence, plans and specifications.

## **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 Confidentiality and IM&T Security 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 and the right to confidentiality in information arises out of contract or common law and judicial precedents.

In respect of commercial confidential information, the means of preservation of the value of information will generally be by explicit contractual provision.

In respect of patient confidentiality the key principle is that where consent has been obtained information should not be used or disclosed further, except as originally understood by the consentor, 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, agency 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<sup>1</sup>. 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 1<sup>st</sup>, requires processing to be fair and lawful and imposes other restrictions;
- the 2<sup>nd</sup>, requires personal data to be processed for one or more specified and lawful purposes;
- the 3<sup>rd</sup>, requires personal data to be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed;
- the 4<sup>th</sup>, requires that data shall be accurate and, where necessary, kept up to date;
- the 5<sup>th</sup>, requires personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose(s);
- the 6<sup>th</sup>, requires that personal data shall be processed in accordance with the rights of the data subjects under the Act;
- the 7<sup>th</sup>, requires personal data to be protected against unauthorised or unlawful processing and against accidental loss, destruction or damage; and
- the 8<sup>th</sup>, 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

---

<sup>1</sup> **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'.

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 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 six 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

## **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.

The SHA has a mandatory obligation under the Information Governance Toolkit to produce a local confidentiality policy.

### References and Further reading:

DoH Confidentiality - NHS Code of Practice

Copies can be downloaded from the Department of Health website: [www.dh.gov.uk](http://www.dh.gov.uk)

GMC – Confidentiality : Protecting and Providing Information

Accessed via the General Medical Council website: [www.gmc-uk.org](http://www.gmc-uk.org)

BMA – Confidentiality & Disclosure of Health Information

Accessed via the British Medical Association website: [www.bma.org.uk](http://www.bma.org.uk)

Confidentiality: What You Need To Know Booklet

Copies can be obtained from the Confidentiality and IM&T Security Helpdesk

NHS Information Governance : Information Security Policy

Copies can be downloaded from the Connecting for Health website: [www.connectingforhealth.nhs.uk](http://www.connectingforhealth.nhs.uk)

### Contact Details:

IT Helpdesk: 0113 295 2190 or 0845 127 2600

**Yorkshire and the Humber Strategic Health Authority**

**Confidentiality Declaration**

**To be completed by all individuals, companies and/or firms to which this Policy applies.**

**Personal Details**

Name:	
Job title:	
Department:	
Address of Organisation / Company (if an Interim Resource, temporary member of staff or secondee):	
Telephone / contact number:	
Name of Line Manager:	

**Declarations**

I confirm that I have read and understood the SHA's Confidentiality Policy Statement and Guidance and agree to adhere to the requirements laid out within it.

I understand that failure to adhere to the policy statement and guidance will be regarded as serious misconduct and may result in the termination of my contact or employment with the SHA or possible legal action being instigated against me or the organisation I work for.

Signed.....Date.....