## Confidentiality and Data Protection Policy

### Document History

<table>
<thead>
<tr>
<th>Version:</th>
<th>V5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ratified by:</td>
<td>(NB: All Procedural Documents which include details of drugs or their management must be approved by the Medicines Management Committee)</td>
</tr>
<tr>
<td>Date ratified:</td>
<td></td>
</tr>
<tr>
<td>Approving Committee/Group (Date):</td>
<td>Information Governance Committee</td>
</tr>
<tr>
<td>Name and Title of originator/author:</td>
<td>Byron Charlton, Information Governance Consultant</td>
</tr>
<tr>
<td>Lead Director:</td>
<td>Helen Astle, Quality Assurance and Governance</td>
</tr>
<tr>
<td>Date issued:</td>
<td>February 2016</td>
</tr>
<tr>
<td>Review due date:</td>
<td>February 2019</td>
</tr>
<tr>
<td>Target audience:</td>
<td>All Staff</td>
</tr>
<tr>
<td>Superseded documents</td>
<td>Confidentiality and Disclosure of Information Policy</td>
</tr>
<tr>
<td>Related CQC Domain</td>
<td>[ ] Safe [ ] Effective [ ] Caring [ ] Responsive [ ] Well-Led</td>
</tr>
<tr>
<td>(Please tick)</td>
<td></td>
</tr>
</tbody>
</table>
| Relevant Standards(e.g. HSE, Health and Social Care Act) | Data Protection Act 1998
NHS Confidentiality Code of Practice
The Caldicott Review 2013
Human Rights Act 2998
Computer Misuse Act 1990
NHS Care Record Guarantee
Common Law Duty of Confidentiality
Administrative Law |

### Acknowledgements

<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
</table>

### Key Words

<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
</table>
## Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Author</th>
<th>Ratified by</th>
<th>Comment/Reason for change</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0</td>
<td>November 2009</td>
<td>Paul Gibbons, Information Governance Manager</td>
<td>Information Governance Committee</td>
<td>Adoption of new template; removal of duplicate material/material covered in other policies (e.g. information security section); incorporation of updated Caldicott Guidelines, Safe Havens procedure and Confidentiality and Data Protection compliance for new processes as appendices; revision of FOIA processes including introduction of FOIA Action Group</td>
</tr>
<tr>
<td>3.1</td>
<td>March 2010</td>
<td>Paul Gibbons, Information Governance Manager</td>
<td>Information Governance Committee</td>
<td>Amendment to charges for subject access requests (Appendix C); addition of 5.1.16 – removal of patient information from Trust property</td>
</tr>
<tr>
<td>3.2</td>
<td>November 2010</td>
<td>Gregory Ugbiyobo, Information Governance Manager</td>
<td>Information Governance Committee</td>
<td>Amendments based on integration with the Community Services and name change for the Trust.</td>
</tr>
<tr>
<td>4.0</td>
<td>November 2011</td>
<td>Gregory Ugbiyobo, Information Governance Manager</td>
<td>Information Governance Committee</td>
<td>Included statement that information may be used in teaching.</td>
</tr>
<tr>
<td>4.1</td>
<td>July 2013</td>
<td>Gregory Ugbiyobo, Information Governance Manager</td>
<td>Information Governance Committee</td>
<td>Amendments based on changes in Management Structure, the law and national guidance. Removal of Confidential Patient Information from Trust premises Caldicott Principles</td>
</tr>
<tr>
<td>5.0</td>
<td>January 2016</td>
<td>Byron Charlton Interim Information Governance Consultant</td>
<td>Information Governance Committee</td>
<td>Reducing the Appendices, taking out duplicate information i.e. Data Protection Act and Caldicott Principles. Further redaction of information that can be found in other appropriate Policies and Procedures.</td>
</tr>
</tbody>
</table>
DOCUMENT STATUS:

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of the document are not controlled.

RELATED DOCUMENTS:

Staff Confidentiality Code of Conduct
Information Governance Strategy and Policy
Information Security Policy
Acceptable Use of Email and Internet Policy
Contents

1  Introduction and aims .............................................................................................................. 5
2.  Scope ..................................................................................................................................... 6
3.  Roles and Responsibilities ................................................................................................. 6
4.  Corporate Level Procedures .............................................................................................. 7
5.  Distribution and Implementation ...................................................................................... 12
6.  Monitoring ............................................................................................................................ 12
7.  Monitoring and review .......................................................................................................... 12
8.  References and Associated Documentation ....................................................................... 12
10.  Discipline ............................................................................................................................. 13
Appendix 1: Confidentiality Dos and Don’ts ................................................................. 14
Appendix 2: Summary of Legal and NHS Mandated Frameworks ......................................... 15
Appendix 3: Reporting of Policy Breaches ............................................................................... 18
Appendix 4: Definitions ............................................................................................................... 19
Appendix 5: Equality Impact Assessment Tool ........................................................................ 20
Appendix 6: Consultation Template ......................................................................................... 21
1. Introduction and Aims

1.1. The purpose of this Data Protection and Confidentiality Policy is to lay down the principles that must be observed by all who work within Croydon Health Services NHS Trust (“the Trust”) and have access to person-identifiable or confidential information. All staff need to be aware of their responsibilities for safeguarding confidentiality and preserving information security.

1.2. The lawful and proper treatment of personal and confidential information is extremely important to the success of the Trust and is vital to maintain the confidence of our service users, employees and customers.

1.3. All employees working in the NHS are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the common law duty of confidence and the Data Protection Act 1998. It is also a requirement within the NHS Care Record Guarantee, produced to assure patients regarding the use of their information.

1.4. It is important the Trust protects and safeguards person identifiable and confidential business information that it gathers, creates, processes and discloses, in order to comply with the law, relevant NHS mandatory requirements and to provide assurance to patients, customers and the public.

1.5. This Policy sets out the requirements placed on all staff when sharing information within the NHS and between NHS and non NHS organisations.

1.6. Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth and NHS number.

1.7. Confidential information within the NHS is commonly thought of as health information; however, it can also include information that is private and not public knowledge or information that an individual would not expect to be shared. It can take many forms including personal confidential data, employee records, occupational health records, etc. It also includes Trust confidential business information.

1.8. Information can relate to patients and staff (including temporary staff), however stored. Information may be held on paper, CD/DVD, USB sticks, computer file or printout, laptops, palmtops, mobile phones, digital cameras or even heard by word of mouth.

1.9. A summary of Confidentiality Do’s and Don’ts can be found at Appendix 1.

1.10. The Legal and NHS Mandated Framework for confidentiality which forms the key guiding principles of this policy can be found in Appendix 2. In particular please note the eight Data Protection Principles.
1.11 How to report a breach of this policy and what should be reported can be found in Appendix 3.

1.12 Definitions of confidential information can be found in Appendix 4.

2.0 Scope

2.1 This Policy applies to anyone who has access to confidential or personal identifiable information, in whatever form, held by the Trust including, permanent and temporary staff, secondees, contracted staff, students/trainees/apprentices voluntary workers. In addition, this policy applies to all third parties and others authorised to undertake work on behalf of the Trust.

3 Roles and Responsibilities

3.1 Chief Executive

The Chief Executive has overall responsibility for strategic and operational management, including ensuring Trust policies comply with all legal, statutory and good practice guidance requirements.

3.2 The Caldicott Guardian

The Caldicott Guardian is the senior responsible person for providing advice on the lawful and ethical processing of personal information of service users and will ensure the appropriate sharing/disclosure of information.

3.3 The Information Governance Committee

The Information Governance Committee is responsible for progressing the agenda on Information Governance encompassing Caldicott Guardianship, Information Governance Management, Data Protection, Informatics and information Security and Confidentiality.

3.4 Director of Human Resources & Organisational Development

The Director of Human Resources & Organisational Development has the responsibility for ensuring the contracts of all staff (permanent and temporary) are compliant with the requirements of this Policy and that confidentiality is included in corporate inductions for all staff.

3.5 Senior Managers

Senior Managers are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance. They must ensure that any breaches of the
policy are reported, investigated and acted upon via the Trust’s Incident Reporting and Management Policy and Procedures.

3.6 All staff

3.6.1 Confidentiality and compliance with data protection requirements is an obligation for all staff and anyone listed in paragraph 2.1. Staff should note that they are bound by the Confidentiality: NHS Code of Practice 2003. There is a Confidentiality clause in contracts and all staff are expected to participate in induction, training and awareness raising sessions carried out to inform and update staff on confidentiality issues.

3.6.2 It is everyone’s responsibility to comply with the most up-to-date version of this policy and it is everyone’s responsibility to ensure that they are aware of the requirements.

3.6.3 Any breach of confidentiality or data protection, inappropriate use of health or staff records, or any personal identifiable or other confidential information, or abuse of computer systems is a disciplinary offence, which could result in dismissal or termination of employment contract. Furthermore, any breach of legal obligations, such as the Data Protection Act 1998, may result in legal proceedings against an individual and/or the Trust.

3.6.4 Where a breach of this Policy has occurred, or a significant risk has been identified, this should be reported to the Line Manager and the Trust’s Serious Incident Reporting Policy.

4 Corporate Level Procedures

4.1 Principles

The principles within the Data Protection 1998 relating to security and confidentiality apply to all Personal Information, which is any information relating to any living individual who can be identified, such as patients, health care professionals, other staff, suppliers, contractors etc. Please note that the Trust will maintain the confidentiality of deceased person’s information and will adhere to the same strict standards, using the Data Protection Act principles as a benchmark.

Such person-identifiable information may be manually-held or automated, and so includes (but is not limited to), for example:

- all patient/service user information;
- personnel records which include those held by line managers and those held centrally by the HR department;
- CCTV videos and other audio/visual recordings;
- Photographs (hard copy or digital), x-rays and other images; and
- computer disks, tapes, CD ROMs and other electronic media
4.1.1 All staff must ensure that the following principles are adhered to:-

- Person-identifiable or confidential information must be effectively protected against improper disclosure when it is received, stored, transmitted or disposed of.
- Access to person-identifiable or confidential information must be on a need-to-know basis.
- Disclosure of person identifiable or confidential information must be limited to that purpose for which it is required.
- 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 concerns about disclosure must be discussed with either your Line Manager or the Information Governance Team. For further details please click on the attached link http://intranet.mayday.nhs.uk/TeamCentre/Corporate/informationgovernance/Pages/home.aspx

4.1.2 That the Trust is responsible for protecting all the information it holds and must always be able to justify any decision to share information.

4.1.3 Person-identifiable information, wherever possible, must be anonymised by removing as many identifiers as possible whilst not unduly compromising the utility of the data.

4.1.4 Access to rooms and offices where terminals are present or person identifiable or confidential information is stored must be controlled. Doors must be locked with keys, keypads or accessed by swipe card. In mixed office environments measures should be in place to prevent oversight of person-identifiable information by unauthorised parties.

4.1.5 All staff should clear their desks at the end of each day. In particular they must keep all records containing person-identifiable or confidential information in recognised filing and storage places that are locked.

4.1.6 Unwanted printouts containing person-identifiable or confidential information must be put into a confidential waste bin. Discs, tapes, printouts and fax messages must not be left lying around but filed and locked away when not in use.

4.1.7 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.
4.2 Disclosing Confidential Information

4.2.1 To ensure that information is only shared with the appropriate people in appropriate circumstances, care must be taken to check they have a legal basis for access to the information before releasing it.

4.2.2 It is important to consider how much confidential information is needed before disclosing it and only the minimal amount necessary is disclosed.

4.2.3 Information can be disclosed:

- When effectively anonymised.

- When the information is required by law or under a Court Order. In this situation staff must discuss this with their Line Manager or Information Governance staff. Approval before sending must be obtained from the Caldicott Guardian.

- In identifiable form, when it is required for a specific purpose, with the individual’s written consent or with support under the Health Service (Control of Patient Information) Regulations 2002 (commonly referred to as a Section 251 Approval), obtained via application to the Confidentiality Advisory Group (CAG) within the Health Research Authority.

- Where disclosure can be justified for another purpose i.e. this is usually for the protection of the public and is likely to be in relation to the prevention and detection of serious crime. In this situation staff must discuss with their Line Manager or Information Governance staff. Approval before sending must be obtained from the Caldicott Guardian.

4.2.4 If staff have any concerns about disclosing information they must discuss this with their Line Manager or the Information Governance staff.

4.2.5 Care must be taken in transferring information to ensure the method used is as secure as it can be. In most instances a Data Sharing, Data Re-Use or Data Transfer Agreement or formal contract will have been completed before any information is transferred. The Agreement/contract will set out any conditions for use and identify the mode of transfer. For further information on Data Sharing Agreements contact the Information Governance team.

4.2.6 Staff must ensure that appropriate standards and safeguards are in place in respect of telephone enquiries, e-mails, faxes and surface mail. See the Safe Haven Procedure for guidance on the safe transfer of confidential or person-identifiable information.

4.2.7 Transferring personal confidential data by email to anyone may only be undertaken by using encryption as per the current NHS Encryption Guidance or through an exchange using the NHS Mail system, (i.e. or from one nhs.net account to another nhs.net account, or from an nhs.net account to a secure...
government domain e.g. gsi.gov.uk), or by using the new encryption functionality for non-NHS mail accounts – See Appendix 1.

4.2.8 Sending information via email to the person to whom the information relates is permissible, provided the risk of using unencrypted email have been explained to them, they have given their consent.

4.3 Working Away from the Office Environment

4.3.1 There will be times when staff may need to work from another location or whilst travelling. This means that staff may need to carry Trust information with them which could be confidential in nature e.g. on a laptop, USB stick or paper documents.

4.3.2 Taking home/removing paper documents that contain person-identifiable or confidential information from Trust premises must obtain your line manager’s approval.

4.3.3 When working away from Trust locations staff must ensure that their working practice complies with Trust’s policies and procedures. Any removable media must be encrypted as per the current NHS Encryption Guidance.

4.3.4 To ensure safety of confidential information staff must keep them on their person at all times whilst travelling and ensure that they are kept in a secure place if they take them home or to another location. Confidential information must be safeguarded at all times and kept in lockable locations.

4.3.5 Staff must minimise the amount of person-identifiable information that is taken away from Trust premises.

4.3.6 If staff do need to carry person-identifiable or confidential information they must ensure the following:

- Any personal information is in a sealed non-transparent container i.e. windowless envelope, suitable bag, etc. prior to being taken out of Trust buildings.
- Confidential information should be kept out of sight whilst being transported (i.e. in the boot of car). Please note that staff must take full responsibility for the information being taken out of the Trust premises.

4.3.7 If staff do need to take person-identifiable or confidential information home they have personal responsibility to ensure the information is kept secure and confidential. This means that other members of their family and/or their friends/colleagues must not be able to see the content or have any access to the information.

4.3.8 Staff must NOT forward any person-identifiable or confidential information via email to their home e-mail account. Staff must not use or store person identifiable or confidential information on a privately owned computer or device on any non-Trust computer or device.
4.4 Carelessness

4.4.1 All staff have a legal duty to keep person-identifiable or confidential information private and not to divulge information accidentally. Staff may be held personally liable for a breach of confidence and must not:

- Talk about person-identifiable or confidential information in public places or where they can be overheard.
- Leave any person-identifiable or confidential information lying around unattended, this includes telephone messages, computer printouts, faxes and other documents, and
- Leave a computer terminal logged on to a system where person identifiable or confidential information can be accessed, unattended.

4.4.2 Steps must be taken to ensure physical safety and security of person identifiable or business confidential information held in any format, such as paper format or any digital form such as on computers or portable electronic devices.

4.4.3 Passwords must be kept secure and must not be disclosed. Staff must not use someone else’s password to gain access to information. Action of this kind will be viewed as a serious breach of confidentiality. This is a disciplinary offence and constitutes gross misconduct which may result in dismissal.

4.5 Abuse of Privilege

4.5.1 It is strictly forbidden for employees to knowingly browse, search for or look at any information relating to themselves, their own family, friends or other persons, without a legitimate purpose. Action of this kind will be viewed as a breach of confidentiality and of the Data Protection Act.

4.5.2 When dealing with person-identifiable or confidential information of any nature, staff must be aware of their personal responsibility, contractual obligations and undertake to abide by the policies and procedures of the Trust.

4.5.3 If staff have concerns about this issue they should discuss it with their Line Manager or Information Governance Team.

4.6 Confidentiality Audits

4.6.1 Good practice requires that all organisations that handle person identifiable or confidential information put in place processes to highlight actual or potential confidentiality breaches in their systems, and also procedures to evaluate the effectiveness of controls within these systems. This function will be coordinated by the Information Governance team through a programme of audits.
5 Distribution and Implementation

5.1 Distribution Plan

5.1.1 This document will be made available to all staff via the Trust intranet site. [http://intranet.mayday.nhs.uk/Documents/PoliciesandProcedure/Forms/InformationGovernance.aspx](http://intranet.mayday.nhs.uk/Documents/PoliciesandProcedure/Forms/InformationGovernance.aspx)

5.1.2 Notice will be sent to all staff notifying them of the release of this document.

5.2 Training Plan

5.2.1 A training needs analysis will be undertaken with staff affected by this document. This is published and reviewed as an appendix to the Information Governance Strategy and Policy.

5.2.2 Based on the findings of that analysis appropriate training will be provided to staff as necessary.

6 Monitoring

6.1.1 Compliance with the policies and procedures laid down in this document will be monitored via the Information Governance team, together with independent reviews by, such as Internal Audit, as deemed necessary by the Information Governance Committee.

6.1.2 The Information Governance Manager is responsible for the monitoring, revision and updating of this document.

7 Monitoring and review

7.1 This Policy will be reviewed every three years unless a change is required because of:

- legislative changes;
- new NHS guidance;
- case law;
- significant incidents reported;
- new vulnerabilities; and
- changes to organisational infrastructure

8 References and Associated Documentation

Staff Confidentiality Code of Conduct
Information Governance Strategy & Policy
Information Security Policy
Acceptable Use of Email and Internet Policy

8.1 All information governance policies and procedures will be made available via the Trust staff intranet
8.2 Staff will be made aware of procedural document updates as they occur via team briefs, team meetings and notification via the Trust staff intranet.

9. **Equality Impact Assessment Statement**

Trust aims to design and implement services, policies and measures that are fair and equitable. As part of its development, this Policy and its impact on staff, patients and the public have been reviewed in line with Trust’s Legal Equality Duties. The purpose of the assessment is to improve service delivery by minimising and if possible removing any disproportionate adverse impact on employees, patients and the public on the grounds of race, socially excluded groups, gender, disability, age, sexual orientation or religion/belief.

The equality impact assessment has been completed and has identified impact or potential impact as 'no impact'.

Trust will endeavour to make sure this Policy supports its diverse workforce look after the information the organisation needs to conduct its business. It will also endeavour to make sure that this information is protected on behalf of patients regardless of race, social exclusion, gender, disability, age, sexual orientation or religion/belief.

10. **Discipline**

**Warning:** Breaches of this Policy will be investigated and may result in the matter being treated as a disciplinary offence under the Disciplinary Policy or in association with the appropriate body which may result in criminal or civil action. Failure to follow a policy could result in disciplinary action being taken, up to and including dismissal.
Appendix 1:

Confidentiality Dos and Don’ts

Do’s

• Do safeguard the confidentiality of all person-identifiable or confidential information that you come into contact with. This is a statutory obligation on everyone working on or behalf of the Trust.
• Do clear your desk at the end of each day, keeping all portable records containing person-identifiable or confidential information in recognised filing and storage places that are locked at times when access is not directly controlled or supervised.
• Do switch off computers with access to person-identifiable or business confidential information, or put them into a password protected mode, if you leave your desk for any length of time.
• Do ensure that you cannot be overheard when discussing confidential matters.
• Do challenge and verify where necessary the identity of any person who is making a request for person-identifiable or confidential information and ensure they have a need to know.
• Do share only the minimum information necessary.
• Do transfer person-identifiable or confidential information securely when necessary i.e. use an nhs.net email account to send confidential information to the following secure government domain i.e.

<table>
<thead>
<tr>
<th>nhs.net</th>
<th>eu-admin.net</th>
<th>pnn.gov.uk</th>
</tr>
</thead>
<tbody>
<tr>
<td>gsi.gov.uk</td>
<td>gsisup.co.uk</td>
<td>scn.gov.uk</td>
</tr>
<tr>
<td>gsx.gov.uk</td>
<td>cjsm.net</td>
<td>pnn.police.uk</td>
</tr>
<tr>
<td>gse.gov.uk</td>
<td>psops.net</td>
<td>gov.uk</td>
</tr>
<tr>
<td>gcsx.gov.uk</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

• Do seek advice if you need to share personal confidential data without the consent of the patient/identifiable person’s consent, and record the decision and any action taken.
• Do report any actual or suspected breaches of confidentiality.
• Do participate in induction, training and awareness raising sessions on confidentiality issues.

Don’ts

• Don’t share passwords or leave them lying around for others to see.
• Don’t share information without the consent of the person to which the information relates, unless there are statutory grounds to do so.
• Don’t use person-identifiable information unless absolutely necessary, anonymise the information where possible.
• Don’t collect, hold or process more information than you need, and do not keep it for longer than necessary.
Appendix 2:

Summary of Legal and NHS Mandated Frameworks

Trust is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of the Trust, who may be held personally accountable for any breaches of information security for which they may be held responsible. Trust staff shall comply with the following legislation and guidance as appropriate:

The Data Protection Act (1998)
Regulates the use of “personal data” and sets out eight principles to ensure that personal data is:

1. Processed fairly and lawfully.
2. Processed for specified and lawful purposes.
3. Adequate, relevant and not excessive.
4. Accurate and where necessary kept up to date.
5. Not kept longer than necessary, for the purpose(s) it is used.
6. Processed in accordance with the rights of the data subject under the Act.
7. Appropriate technical and organisational measures are be taken to guard against unauthorised or unlawful processing, accidental loss or destruction of, or damage to, personal data.
8. Not transferred to countries outside the European Economic Area (EEA) without an adequate level protection in place.


https://ico.org.uk/

Recommended that a series of principles be applied when considering whether confidential patient-identifiable information should be shared:

- Justify the purpose for using patient-identifiable information.
- Don’t use patient identifiable information unless it is absolutely necessary.
- Use the minimum necessary patient-identifiable information.
- Access to patient-identifiable information should be on a strict need to know basis.
- Everyone should be aware of their responsibilities.
- Understand and comply with the law.

An additional principle is recommended in the 2013 Caldicott information governance review titled Information: To Share or Not to Share:

- The duty to share information can be as important as the duty to protection patient confidentiality.

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by
these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Click here for an online link to The Caldicott Report 1997

Click here for an online link to The Caldicott Review 2013

**Article 8 of the Human Rights Act (1998)**
Refers to an individual's “right to respect for their private and family life, for their home and for their correspondence”. This means that public authorities should take care that their actions do not interfere with these aspects of an individual’s life.

Click here for an online link to the Human Rights Act 1998

**The Computer Misuse Act (1990)**
Makes it illegal to access data or computer programs without authorisation and establishes three offences:

1. Unauthorised access data or programs held on computer e.g. to view test results on a patient whose care you are not directly involved in or to obtain or view information about friends and relatives.
2. Unauthorised access with the intent to commit or facilitate further offences e.g. to commit fraud or blackmail.
3. Unauthorised acts the intent to impair, or with recklessness so as to impair, the operation of a computer e.g. to modify data or programs held on computer without authorisation.

Click here for an online link to the Computer Misuse Act 1990

**The NHS Confidentiality Code of Practice (2003)**
Outlines for main requirements that must be met in order to provide patients with a confidential service:

- Protect patient information.
- Inform patients of how their information is used.
- Allow patients to decide whether their information can be shared.
- Look for improved ways to protect, inform and provide choice to patients.

Click here for an online link to NHS Confidentiality Code of Practice 2003

**Common Law Duty of Confidentiality**
Information given in confidence must not be disclosed without consent unless there is a justifiable reason e.g. a requirement of law or there is an overriding public interest to do so.

**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.
The NHS Care Record Guarantee
The Care Record Guarantee sets out twelve high-level commitments for protecting and safeguarding patient information, particularly in regard to: patients’ rights to access their information, how information will be shared both within and outside of the NHS and how decisions on sharing information will be made. The most relevant are:

Commitment 3 - We will not share information (particularly with other government agencies) that identifies you for any reason, unless:
- You ask us to do so.
- We ask and you give us specific permission.
- We have to do this by law.
- We have special permission for health or research purposes; or
- We have special permission because the public good is thought to be of greater importance than your confidentiality, and
- If we share information without your permission, we will make sure that we keep to the Data Protection Act, the NHS Confidentiality Code of Practice and other national guidelines on best practice.

Commitment 9 - We will make sure, through contract terms and staff training, that everyone who works in or on behalf of the NHS understands their duty of confidentiality, what it means in practice and how it applies to all parts of their work. Organisations under contract to the NHS must follow the same policies and controls as the NHS does. We will enforce this duty at all times.

Click here for an online link to NHS Care Record Guarantee
Appendix 3:

Reporting of Policy Breaches

What should be reported?

Misuse of personal data and security incidents must be reported so that steps can be taken to rectify the problem and to ensure that the same problem does not occur again.

All breaches should be reported through the Trust’s Serious Incident Reporting Policy. If staff are unsure as to whether a particular activity amounts to a breach of the policy, they should discuss their concerns with their Line Manager or Information Governance staff. The following list gives examples of breaches of this Policy which should be reported:

- Sharing of passwords.
- Unauthorised access to Trust systems either by staff or a third party.
- Unauthorised access to person-identifiable information where the member of staff does not have a need to know.
- Disclosure of person-identifiable information to a third party where there is no justification and you have concerns that it is not in accordance with the Data Protection Act 1998 and NHS Code of Confidentiality.
- Sending person-identifiable or confidential information in a way that breaches confidentiality.
- Leaving person-identifiable or confidential information lying around in public area.
- Theft or loss of person-identifiable or confidential information.
- Disposal of person-identifiable or confidential information in a way that breaches confidentiality i.e. disposing off person-identifiable information in an ordinary waste paper bin, or non-secure disposal of devices containing person-identifiable or confidential information.

Seeking Guidance

It is not possible to provide detailed guidance for every eventuality. Therefore, where further clarity is needed, the advice of a Senior Manager or Information Governance staff should be sought.

Reporting of Breaches

Breaches of confidentiality of person-identifiable or confidential information will be reported to the Information Governance Steering Group. The information will enable the monitoring of compliance and improvements to be made to the policy and procedures.
Appendix 4:

Definitions

The following types of information are classed as confidential. This list is not exhaustive:

Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number, National Insurance number etc. Even a visual image (e.g. photograph) is sufficient to identify an individual. Any data or combination of data and other information, which can indirectly identify the person, will also fall into this definition.

Sensitive personal information as defined by the Data Protection Act 1998 refers to personal information about:

- Race or ethnic origin
- Political opinions
- Religious or similar beliefs
- Trade union membership
- Physical or mental health or condition
- Sexual life
- Commission or alleged commission of any offence, or
- Any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings

Non-person-identifiable information can also be classed as confidential such as confidential business information e.g. financial reports; commercially sensitive information e.g. contracts, trade secrets, procurement information, which should also be treated with the same degree of care.
### Appendix 5: Equality Impact Assessment Tool

<table>
<thead>
<tr>
<th>An Organisation-wide Document for the Development and Management of Procedural Documents</th>
<th>Yes/No</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. Does the document affect one group less or more favourably than another on the basis of:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Race</td>
<td>Y/N</td>
<td></td>
</tr>
<tr>
<td>• Ethnic origins (including gypsies and travellers)</td>
<td>Y/N</td>
<td></td>
</tr>
<tr>
<td>• Nationality</td>
<td>Y/N</td>
<td></td>
</tr>
<tr>
<td>• Gender</td>
<td>Y/N</td>
<td></td>
</tr>
<tr>
<td>• Culture</td>
<td>Y/N</td>
<td></td>
</tr>
<tr>
<td>• Religion or belief</td>
<td>Y/N</td>
<td></td>
</tr>
<tr>
<td>• Sexual orientation including lesbian, gay and bisexual people</td>
<td>Y/N</td>
<td></td>
</tr>
<tr>
<td>• Age</td>
<td>Y/N</td>
<td></td>
</tr>
<tr>
<td><strong>2. Is there any evidence that some groups are affected differently?</strong></td>
<td>Y/N</td>
<td></td>
</tr>
<tr>
<td><strong>3. Is there a need for external or user consultation</strong></td>
<td>Y/N</td>
<td></td>
</tr>
<tr>
<td><strong>4. If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?</strong></td>
<td>Y/N</td>
<td></td>
</tr>
<tr>
<td><strong>5. Is the impact of the policy/guidance likely to be negative?</strong></td>
<td>Y/N</td>
<td></td>
</tr>
<tr>
<td><strong>6. If so can the impact be avoided?</strong></td>
<td>Y/N</td>
<td></td>
</tr>
<tr>
<td><strong>7. What alternatives are there to achieving the policy/guidance without the impact?</strong></td>
<td>Y/N</td>
<td></td>
</tr>
<tr>
<td><strong>8. Can we reduce the impact by taking different action?</strong></td>
<td>Y/N</td>
<td></td>
</tr>
</tbody>
</table>
### Appendix 6: Consultation Template

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Procedural Document’s Name:</td>
</tr>
<tr>
<td>2</td>
<td>Procedural Document Author:</td>
</tr>
<tr>
<td>3</td>
<td><strong>Group/Committee Consulted</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><strong>Name and Title of Key Individuals Consulted</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Comments received</td>
</tr>
</tbody>
</table>
