

**NHS Waltham Forest**  
**Clinical Commissioning Group**  
**Confidentiality and Disclosure of**  
**Information Policy**

Author:	Zeb Alam (NELCSU) / David Pearce
Version:	3.0
Amendments to Version 2.0 <ul style="list-style-type: none"> <li>- Minor changes to incorporate Caldicott2 recommendations and to reference the re-use of Public Sector Information Regulations</li> <li>- Examples of NHS protective markings included</li> <li>- Proposed review of policy after 2 years or earlier if changes in legislation or national guidance warrant an earlier review</li> </ul>	Amendments made by: Zeb Alam (NELCSU) / David Pearce
Review date:	October 2017

## Contents

1. Summary	3
2. Scope	3
3. Introduction	3
4. Purpose	4
5. Roles and Responsibilities	4
6. Policy Standards	6
7. Disclosures of Information	8
8. Consent to Share Information	11
9. Caldicott Compliance	13
10. Anonymisation and Pseudonymisation	13
11. Sharing of Personal Information & Transfer of Data / Information	14
12. Training Requirements	15
13. Relationship with Service providers	15
14. Equality and Diversity	16
15. Dissemination and Implementation	16
16. Non conformance to this policy	16
17. Monitoring and Review	16
18. Compliance standards	17

## Appendices:

Appendix A: Evaluation protocol

Appendix B: Equality and Equity Impact Assessment

Appendix C: Definitions

Appendix D: Confidentiality and Information Sharing Quick Reference Guide

Appendix E: Disclosure Model where it is proposed to share confidential information in order to provide healthcare

Appendix F: Disclosures for non healthcare provision but a medical purpose in legislation

Appendix G: Disclosures unrelated to healthcare or another medical purpose

## 1. Summary

Waltham Forest Clinical Commissioning Group (CCG) has put this policy in place to ensure staff are fully aware of their responsibilities when collecting and using confidential information. This policy is important as it should help you understand how to effectively maintain compliance with confidentiality and Data Protection Act when handling information needed to fulfil your role consistent with the law and expected standards.

Information is a valuable asset to a commissioning organisation to enable it to effectively make informed decisions. Therefore it is important to ensure we maximise the value of information as an 'asset' in compliance with legal requirements. To do this we will ensure information is:

- Held securely and confidentially;
- Obtained fairly and lawfully;
- Recorded accurately and reliably;
- Used effectively and ethically; and
- Shared and disclosed appropriately and lawfully.

The CCG is committed to ensuring that information, in whatever its context, is processed as determined by prevailing law, statute and best practice. Compliance with all organisation policies is a condition of employment and a breach of policy may result in disciplinary action.

## 2. Scope

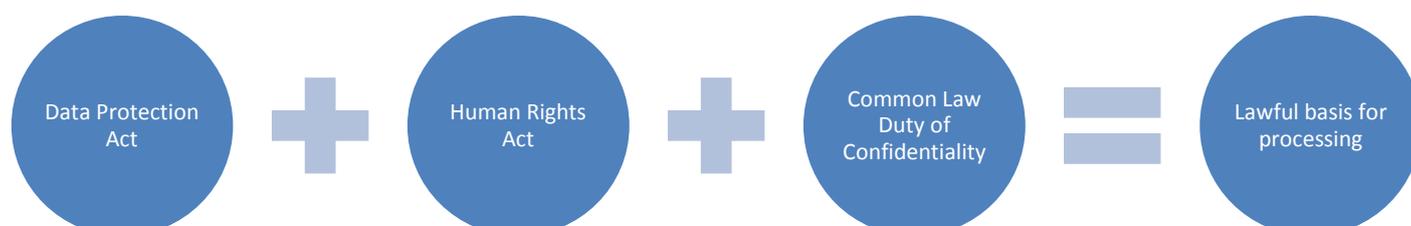
This policy covers all aspects of compliance with confidentiality, data protection and when holding, obtaining, recording, using, sharing and disclosing of data/information or records, held in a manual/paper or electronic format, by or on behalf of the CCG.

This includes, but is not limited to; staff employed by the organisation; those engaged in duties for the organisation under a letter of authority, honorary contract or work experience programme; volunteers and any other third party such as contractors, students or visitors.

## 3. Introduction

The CCG will hold some personal and confidential data relating to patients, the public and its employees. With ever-easier ways by which information can be accessed and shared it is important that a consistent approach is adopted to safeguard the organisation information as an asset.

It is recognised as a commissioner that access to personal confidential data will be limited but may on occasion happen. Any collection or use of such data will need to comply with:



The CCG, as a commissioner, will not always have the primary contact who collected information and therefore it would be this first interaction with the data source that needs to be considered when trying to establish the expected level of confidentiality

#### 4. Purpose

The Policy is intended to achieve and maintain the following Information Governance objectives:

##### Confidentiality

- assuring that sensitive information or data is accessible to only authorised individuals, and is not disclosed to unauthorised individuals or the public unless appropriate and lawful.

##### Integrity

- safeguarding the accuracy and completeness of information and software, and protecting it from improper modification.

##### Availability

- ensuring that information, systems, networks and applications as well as paper records are available when required to departments, groups or users that have a valid reason and authority to access them.

##### Accountability

- users will be aware of their responsibilities in relation to their collection, use and processing of data and information.

#### 5. Roles and responsibilities

Confidentiality is everybody's business and therefore it is everybody's responsibility to ensure information is processed appropriately. This section describes the expected responsibilities in relation to Information Security of persons processing information. It is noted that some individuals will hold more than one role.

Role	Responsibilities
Governing Body	<p>In line with the <a href="#">Guidance for NHS Boards: Information Governance</a>, the governing body will ensure that its organisation has taken appropriate steps to meet IG standards. In particular it will seek assurance against following questions:</p> <ol style="list-style-type: none"><li>1. "What have we done, as an organisation, to ensure we have implemented adequate policies and procedures, and are addressing the responsibilities and key actions required to support effective IG?"</li><li>2. "What were the outcomes of our most recent annual IG assessment, and what measures (if any) have been put in place to address any identified deficiencies?"</li><li>3. "What plans do we have in place to ensure our organisation remains compliant with national standards for IG?"</li><li>4. "Do we as an organisation have the capacity and capability to guarantee our plans for IG can be implemented?"</li><li>5. "Do our IG arrangements adequately encompass all teams and work areas that we are legally accountable for?"</li><li>6. "What plans do we have in place to ensure compliance with the Caldicott 2 recommendations?"</li><li>7. "What plans do we have for protected disclosures as a result of the Public Sector Information Regulations 2015?"</li><li>8. "Are all significant IG Risks being managed effectively and considered at an appropriate level? Have there been any serious incidents requiring investigation reported? "</li></ol>
Accountable Officer	<p>Has overall accountability and responsibility for governance within the organisation. Is to provide assurance that all risks to the organisation, including those relating to information, are effectively managed and mitigated.</p>

Role	Responsibilities
Senior Information Risk Owner (SIRO)	<p>Has overall responsibility for ensuring that effective systems and processes are in place to address the IG agenda.</p> <ul style="list-style-type: none"> <li>• Foster a culture for protecting and using data.</li> <li>• Ensure information risk requirements are included in the corporate Risk and Issue Management Policy.</li> <li>• Ensure Information Asset Owners (IAOs) undertake risk assessments of their assets.</li> <li>• Be responsible for the Incident Management process ensuring identified information security risks are followed up, incidents managed and lessons learnt.</li> <li>• Provide a focal point for the management, resolution and/or discussion of information risk issues.</li> <li>• Ensure that the CCG's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff.</li> <li>• Ensure the Governing Body is adequately briefed on information risk issues.</li> <li>• Be accountable for information risk.</li> </ul> <p>The SIRO roles and responsibilities are defined in <a href="#">Appendix A of the NHS Information Risk Management Guidance</a>. The role holder will be supported and advised by the IG Team.</p>
Caldicott Guardian	<p>The role of the Caldicott Guardian is an advisory role acting as the conscience of the organisation for management of patient information and a focal point for patient confidentiality &amp; information sharing issues.</p> <p>To ensure that the CCG completes all requirements in the Caldicott plan relevant to the CCG</p> <p>The Caldicott Guardian is supported in this role by the IG Lead and IG Team who provide the Caldicott Function for the organisation.</p> <p>To be informed of the final IG Toolkit submission status for the CCG as the Caldicott assurance and compliance report are then available from the IG Toolkit.</p>
Information Asset Owners	<p>All senior staff at Director level are required to act as Information Asset Owners for the information assets within their remit. They will provide assurance to the SIRO that information risk is managed effectively for the information assets identified as within their remit. They will also:</p> <ul style="list-style-type: none"> <li>• Ensure all Information Assets and flows of data within their remit are identified and logged ensuring each has a legal basis to be processed.</li> <li>• Identify, manage and escalate all information security (for example, dependencies and access control) and information risks as appropriate.</li> </ul> <p>The IAOs will be supported by IAAs who will ensure the above takes place. The detailed roles and responsibilities are defined in <a href="#">Appendix A of the NHS Information Risk Management Guidance</a></p>
Information Asset Administrators	<p>Information Asset Administrators (IAAs) are the most senior individual user or direct users of systems and have an understanding as to how they work and how they are used.</p> <p>They will ensure there are procedures for using them, control access to them and understand their limitations. The detailed roles and responsibilities are defined in <a href="#">Appendix A of the NHS Information Risk Management Guidance</a></p>
Information Governance Lead	<p>Senior CCG Manager responsible for ensuring suitable advice, guidance support, tools and training are available to those with the CCG who handle data, to ensure they do so appropriately. This role will be the main point of contact for the NEL CSU IG Team.</p>

Role	Responsibilities
NEL CSU IG Team	Provide specialist advice and support, under contract, to the organisation in relation to IG subject matters. They will also form part of the Caldicott function.
All Substantive/Permanent Staff	All those working for the CCG have legal obligations, under the Data Protection Act and common law of confidentiality; and professional obligations, for example the <a href="#">Confidentiality NHS Code of Practice</a> and professional codes of conduct to manage information appropriately. These are in addition to their contractual obligations which include adherence to policy, and confidentiality clauses in their contract.
Third parties	The same responsibilities as for permanent staff apply to those working on behalf of the organisation, whether they are volunteers, students, work placements, contractors or temporary employees. Those working on behalf of, but not directly employed by, the organisation are required to sign a third party agreement outlining their duties and obligations.
CCG Member Practices	This policy should be followed where any member is processing information on behalf of or in relation to the CCG delivery of its functions. However it is recommended that similar policy standards are in place within each member practice regarding the management of its own data and information.
Managers	All staff with a management or supervisory role have a responsibility to ensure that all staff have been shown how to access this and related policy, supporting guidance and training.

## 6. Policy Standards

This policy document, as part of a suite of supporting Information Governance related policies, sets out the standards that those working for or on behalf of the CCG are expected to adhere to when handling data or information.

### 6.1. Accountability and Governance

The CCG will put in place suitable controls to:

- Assign responsibilities to oversee the delivery of standards set out in this policy
- Report on compliance against Information Governance to a suitable committee within the organisation
- Ensure that all staff have been made aware of their responsibilities, how to comply with them and have available advice and guidance and training programmes to do so
- ensuring the consistency of information governance across the organisation;
- develop information governance policies and procedures;
- ensuring compliance with Data Protection, and other information security related legislation;
- providing support to the Caldicott Guardian and Senior Information Risk Owner (SIRO).

### 6.2. Managing Information Risk

The CCG will put in place suitable mechanisms to ensure staff identify and manage information risks in line with existing risk management policy and processes. A failure to effectively implement information could lead to the following risks.

Risk	Example
<b>Reputational Damage</b>	<ul style="list-style-type: none"> <li>making decisions from inaccurate information could undermine any commissioning decision and be challenged could affect organisational reputation</li> </ul>
<b>Financial Loss</b>	<ul style="list-style-type: none"> <li>Loss of information could lead to financial penalties of up to £500,000</li> <li>Inefficient use of information may lead to duplication and wasted time</li> </ul>
<b>Failure to comply with legal, regulatory or NHS requirements</b>	<ul style="list-style-type: none"> <li>There are a number of lawful requirements to manage information such as the Data Protection Act, Freedom of Information Act, , Public Sector Information Regulations 2015 which could also lead to reputation or financial loss</li> <li>Failure to be compliant with <a href="#">NHS Constitution</a> or <a href="#">NHS Care Records Guarantee</a> or CCG Authorisation requirements.</li> </ul>

CCG Information Asset Owners ([IAOs](#)) must ensure that information assets are assessed for risk, regularly in line with Risk Management Policy and guidance. Results of risk assessments should be placed on risk registers and escalated as per the Risk Management Policy and guidance.

### 6.3. Confidentiality

A duty of confidence arises when one individual discloses information to another where is expected that the information will be held in confidence. It is:

- a legal obligation
- established within professional coded of conduct
- a requirement within employment and service contracts

#### Patient Confidentiality (NHS Confidential)

All patients, carers and staff should be able to expect that any information given to any member of staff within the Trust will be held in a secure and confidential manner and will not be divulged to others without their express permission except in the following circumstances:

- it is with the consent of the individual or by law of the order of a court
- necessary in the public interest including the protection of a child
- assuring and improving quality of care and treatment (e.g. clinical audit)
- investigating complaints or potential legal claims
- for the purposes of direct care, relevant personal confidential data can be shared among the registered and regulated health and social care professionals who have a legitimate relationship with the individual.

Any member of staff who is in doubt should consult their Line Manager.

#### Staff Confidentiality (NHS Confidential)

Personal information about members of staff must be regarded as confidential at all times. This includes information such as:

- Illness
- Current or previous disciplinary procedures
- Employment references

- Personal living arrangements such as family life and sexuality
- Home address and telephone number
- Any other information which has been given in confidence

The Trust will ensure there are adequate procedures in place to protect against the unauthorised processing of information and against accidental loss, destruction and damage to this information. See the Information Security Policy.

### **Confidential business information (NHS Protect)**

Information used for the planning and delivery of business services may be regarded as confidential. Although the majority of corporate information relating to the CCG is available under the Freedom of Information Act there may be certain exemptions to this. Where the release of the information would compromise the commercial interests of the CCG the information should not be released. For more information and guidance on the release of business information please discuss with the IG and FOI teams.

## **7. Disclosures of Information**

This policy will formally adopt the guidelines set out [Confidentiality: NHS Code of Practice \(2003\)](#) set out by the Department of Health.

The Trust will follow the principles of information disclosure as laid down by the [Confidentiality: NHS Code of Practice \(2003\)](#). The Code is relevant to any one working in and around health and social care. In particular how to make decisions regarding the disclosure of NHS Confidential Information (Appendix 2)

### **Disclosures for Health and Social Care purposes**

Whilst a commissioner of service the CCG will not generally have a role in the day to day sharing of information to support direct care provision although it may facilitate data sharing agreements, for example, between parties from whom it commissions services and the GPs in its area. In circumstances where this is the case any collection and disclosure would be in line with this policy and be limited to

- To NHS staff involved in the provision of healthcare (Limited to relevant persons only)
- To social workers or other non-NHS staff involved in the provision of healthcare (Limited to relevant persons only)
- parents, i.e. those with parental responsibility for patients, and guardians
- To carers without parental responsibility to the extent necessary for care.

Particular attention should be given to:

#### **Parents, i.e. those with parental responsibility for patients, and guardians**

Those children competent to consent to treatment will be entitled to the same duty of confidence as adults, and their consent is required to disclose and use information. Staff should encourage those children to involve parents, particularly where making significant decisions, however should respect the choice made. In situations involving refusal of treatment in life threatening situations, disclosure may be appropriate. See the consent to treatment policy for further information.

#### **To carers without parental responsibility**

Only information essential to a patient's care should be disclosed and patients should be made aware that this is the case. However, the explicit consent of a competent patient is needed before disclosing information to a carer. The best interests of a patient who is not competent to consent may warrant disclosure.

### **Disclosures for Audit and Investigation purposes**

- Clinical audits should not normally require disclosure of Personal Confidential Data. Where this is deemed necessary guidance should be sought from the relevant source of IG advice and the CCG Caldicott Guardian.
- Investigations may require the provider to have access to the relevant data, but ordinarily there should be no requirement to disclose this level of detail to the CCG.

### **Disclosures for non-healthcare provision but a medical purpose in legislation**

There are a number of work activities that are required for the organisation to carry out its functions that are legally defined as a medical purpose. For using or collecting information where the activities below are carried out, in most cases reliance will be placed on receiving explicit consent, Otherwise anonymised or pseudonymised data must be used for such purposes. The purposes concerned are:

- To researchers
- To NHS managers and the Department of Health, e.g. commissioning, prescribing advisors, financial audit, resource allocation etc.
- To Occupational Health professionals
- Complaints processes
- Cancer registries (Currently have legal gateway for disclosure without consent)

It is not always practical to obtain this consent however unless there is a legal power that enables disclosure without consent in place (e.g. under the regulations made under Section 251 of the NHS Act 2006 or bodies with statutory investigative powers) the disclosure must not take place.

It is however the organisations position that anonymised or pseudonymised information may be used in so much as it no longer becomes personal data. The NHS Number must not be used as the pseudonymised key as it can easily be used to identify individuals.

### **Disclosures unrelated to healthcare or another medical purpose**

There are a number of other situations that may require information to be disclosed, where you would ordinarily rely on consent to release unless exceptional circumstances exist. These circumstances have been explained in further detail within appendix B. Such examples include disclosures to:

- Religious persons e.g. chaplains or priests
- Non- statutory investigations, e.g. Members of Parliament
- Government departments (excluding the Department of Health for Healthcare purposes)
- The police
- The courts, including a coroner's court, tribunals and enquiries
- Sure Start Teams, Children's Centres or equivalent
- The media
- Solicitors

#### **7.1. Informing individuals about the uses of information**

The CCG will ensure compliance with Data Protection Act Requirement that individuals are appropriately informed about the use, including disclosure, of their information

As a commissioner the CCG will need to ensure any flow of data from a provider is compliant with this requirement which forms part of a contractual obligation. As such the Health Professional(s) involved in their care, will communicate any changes of use of their personal information to the patient. Patients will either be informed verbally or in writing, depending on the nature of changes.

Staff will be informed by their line managers about the use of their information.

#### **7.2. Information Assets & Register**

Information as with any other assets of the organisation should be seen and recorded as an asset, which can take many forms. For the purpose of this policy the key assets that Information Asset Owners ([IAOs](#)) should be identifying are those which contain:

- Records containing personal information such as HR and patient information and electronic systems with the data within records

Software and non-portable hardware assets will be recorded by the IT Service and people recorded by Human resources.

Once information assets have been identified, the [IAOs](#) must log each on a local register and identify associated assets along with the risks and corresponding controls

Where suitable controls are not in place an action plan is to be agreed with the relevant [IAO](#), [IAA](#) and IG Team on behalf of the SIRO to address any shortfalls and risks recorded on the corporate risk register.

### 7.3. Data/Information Classification

Information assets should be classified using the adapted NHS national classification scheme. Previous to this policy all information assets were classified and marked according to the following terms.

Marking	Description
<b>NHS Confidential</b>	This is appropriate for documents and files containing person-identifiable clinical or staff information given in confidence not for general disclosure. Access should be tightly controlled and restricted.
<b>NHS Protect or Restricted</b>	This applies to corporate records where the basic principles would be to handle with care, restrict disclosure and secure.
<b>NHS Public</b>	Any information which does not warrant being marked with one of the above classifications is to be marked NHS Public. These records should be considered to be open and routinely made available to the public.

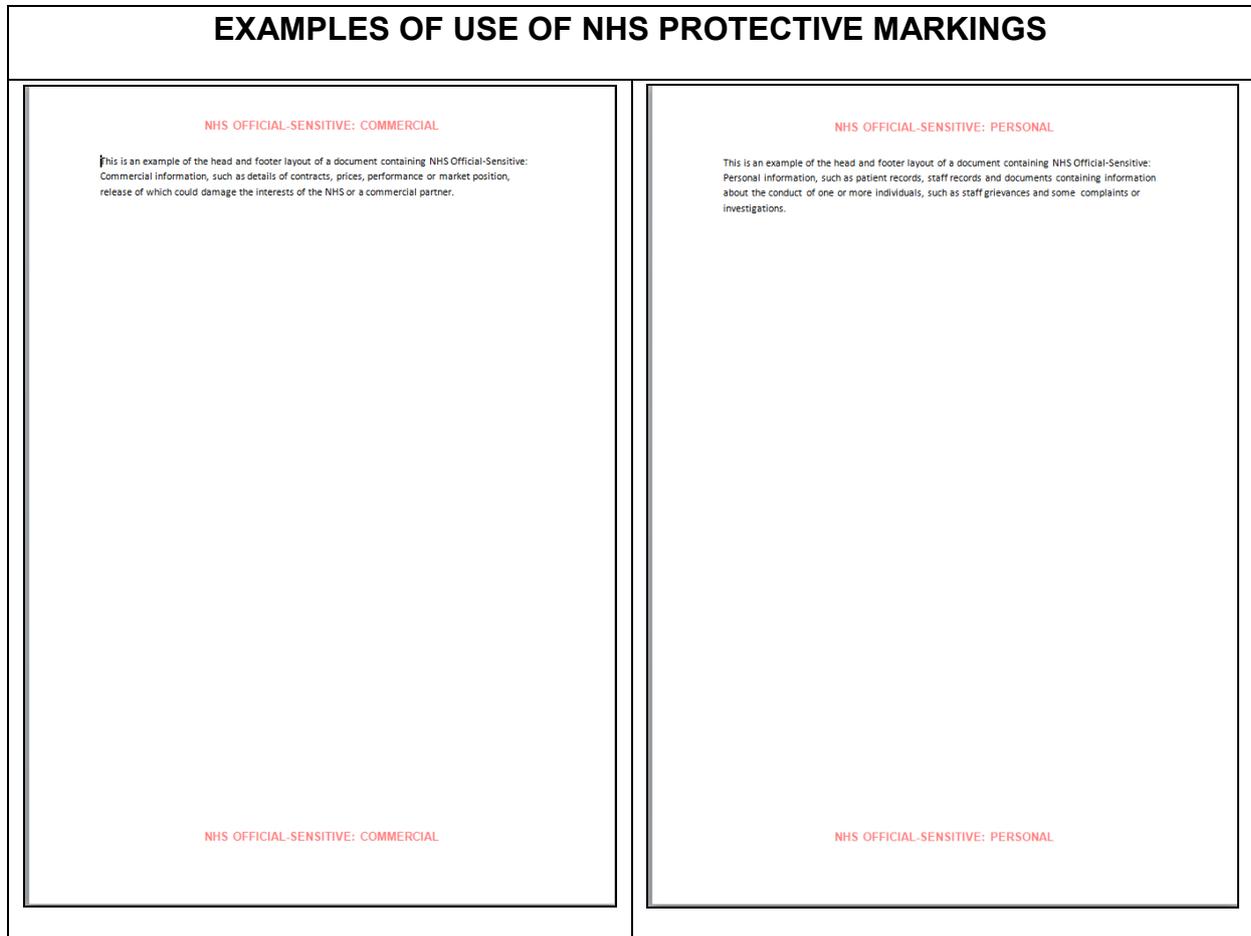
With effect from April 2014, new Government Security markings have been introduced to replace these markings. This does not apply retrospectively.

Marking	Description
<b>NHS Official</b>	All routine CCG business, operations and services should be treated as OFFICIAL. The subset categories of OFFICIAL-SENSITIVE: COMMERCIAL and OFFICIAL-SENSITIVE: PERSONAL should be used where applicable. Ordinarily NHS Official information does not need to be marked.
<b>NHS Official-Sensitive</b>	This marking is necessary for person-identifiable information and commercially sensitive information and is applicable to paper and electronic documents/records.
<b>NHS Official-Sensitive: Commercial</b>	Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to the CCG, other NHS body or a commercial partner if improperly accessed.
<b>NHS Official-Sensitive: Personal</b>	Personal information relating to an identifiable individual where inappropriate access could have damaging consequences.

Where existing information is marked NHS Confidential it should be be treated as NHS Official: Sensitive

NHS Official-Sensitive (including NHS Official – Sensitive: Commercial and NHS Official – Sensitive: Personal Information should be secured using the standards set out in this policy for as long as they are held until securely disposed of.

Examples of the use of the markings are shown below:



#### 7.4. Information Security incident management

All staff are responsible for ensuring that any actual or potential Incidents are reported in line with the WFCCG Incident Reporting policy which include actual or suspected breaches of confidentiality as outlined in the Information Security Policy.

#### 8. Consent to sharing information

It is CCG policy that in all but exceptional cases, where law permits, individuals will be informed about and consent to their information being collected, used, stored and shared.

Everyone aged 16 or over is presumed to be competent to give consent for themselves unless the opposite is demonstrated. Those under 16 years old who have the capacity and understanding to make decisions about their treatment are entitled also to decide on the use of their personal information.

In the case of those without capacity, every effort should be made to obtain consent from the individual concerned or individual with legal responsibility for the care of the individual e.g. parent or guardian. The decision to share information without consent must take into consideration the patient's best interests as with consent to treatment. All such decisions should be documented.

## **For Health and Social Care purposes**

It is impracticable to obtain explicit written consent of the patient every time that health care information needs to be shared with another health professional, or other staff involved in the health care of that patient (Section 4.1 of this policy). Consent in these instances can be implied provided that it is known and understood by the patients that such information needs to be made available to others involved in the delivery of their care from the onset. Consent is required if the purposes for which the collection of the information changes.

To inform patients correctly staff should:

- Check where practicable that information leaflets on patient confidentiality and information disclosure have been given to the patient, read and understood.
- Make clear to patients when information is recorded or health records are accessed including who they are or who they will be disclosing information to.
- Check patients are aware of choices of how their information may be disclosed and used ensuring they have no concerns or queries.
- Answer any queries personally or direct the patient to others who can answer their questions.
- Respect the right of patients including their right to have access to their health records.

## **Non healthcare disclosures**

Many proposed uses of confidential patient information do not directly contribute to or support the healthcare that a patient receives. It cannot be assumed that patients will consent for their information to be used in these ways. It is therefore required that, unless a legal requirement to disclose without consent, the following should take place:

- Individuals are asked before using their personal information in ways that do not directly contribute to or support the delivery of their care
- Respect individuals decisions to restrict the disclosure or use of information except where exceptional circumstances apply (see appendix B models 2 and 3)

## **Withholding consent**

In some cases, it may not be possible to restrict information disclosure without compromising care. This should be discussed with the patient, explaining fully the consequences of refusal.

It is essential that complete records are kept of all care provided and of any restrictions placed on disclosing information by patients. If patients impose constraints, it is important to demonstrate that neither patient safety, nor clinical responsibility for healthcare provision, has been neglected.

## **Disclosures in the Public Interest**

In certain exceptional circumstances an individual's right to confidentiality may be overridden by the public's interest in having access to the information, for example where it may prevent or detect serious crime.

Such decisions must not be taken lightly, and should be made by the health care professional concerned. This should occur following consultation with fellow practitioners and with their line manager.

It must be noted there may be ramifications and these are best explored before a final decision as to whether to withhold or disclose information is made. Advice and guidance may also be obtained from the Information Governance department or Caldicott Guardian. Furthermore, it may on some occasions be appropriate to seek legal advice.

All decisions should be appropriately documented in the appropriate record or in a separate note that can be kept on an individual's file.

## Investigation of Complaints

Implied consent can be applied in the use of a patient's personal information to investigate a complaint. This only applies to information relevant to the investigation of the complaint and only disclosed to those people who have a demonstrable need to know it for the purpose of investigating the complaint or incident.

It must be explained to the patient that information from their health records may need to be disclosed to the manager handling the complaint, to clinical assessors, and any others likely to access the information. If the patient objects to this, then the effect on the investigation will need to be explained. The patient's wishes should always be respected unless there is an overriding public interest in continuing with the matter.

Where a complaint is made on behalf of a patient who has not authorised someone to act for them, care must be taken not to disclose personal health information to the complainant, unless the patient has expressly consented to its disclosure.

## 9. Caldicott Compliance

It is important to minimise the amount of information to only that which is absolutely required. It is important to consider how much information is needed before disclosing it. When seeking to share the minimum amount of information, it is important to:

- Justify the purpose (to be undertaken by staff irrespective of whether it is due to a request to provide information or to receive information from another source);
- Do not use patient identifiable information unless it is absolutely necessary;
- Use the minimum necessary patient identifiable information;
- Ensure that access to patient identifiable data and information occurs on a strict 'need to know' basis;
- Be aware of all relevant policies and their responsibilities
- Understand and comply with the law
- Remember the duty to share can be as important as the duty to protect patient confidentiality . (for direct patient care)

## 10. Anonymisation and pseudonymisation

It is recognised that the organisation is required to manage and plan services; this will be considered a secondary use of information that has been collected and require consent to process. It is therefore expected that such information will be either anonymised or pseudonymised to allow this to take place without identifying the individual concerned.

Anonymisation itself does not allow long term management and planning therefore pseudonymisation will be the preferred option which will mean. All systems will be required to:

1. Provide a unique pseudonymised key that a recipient would only be able to re-identify by returning to the organisation
2. Remove Demographics and provide the following:
  - a. Age instead of date of birth
  - b. The first half of postcode a postcode (and up to the first character of the second half)
  - c. lower Superannuated output area (if possible)
3. Conduct a risk assessment to identify the likelihood of re-identification based upon the information contained within the data, the potential information the recipient has and what is also available in the public domain in line with [Anonymisation Standard for Publishing Health and Social Care Data](#)

## 11. Sharing of Personal Information & Transfer of data/information

The transfer of any information using the previous classifications of [NHS Confidential](#) or [NHS Protect or Restricted](#) information must:

1. Be reviewed and a lawful basis established to transfer it
2. Follow the principles and underpinning guidance to maintain the security of the information in transit.

### 11.1. Data Flow Mapping

Routine transfers should be logged regardless of size to allow review of security procedures in place and compliance with Information Governance requirements. [IAOs](#) are required to identify and log the routine transfers of data that will take place including

- Lawful basis
- Use of approved method
- Volume
- Frequency
- Risks
- Compensating controls

### 11.2. Information Sharing Agreements

The organisation will enter into information sharing agreements with relevant organisations to formally document routine transfers of information. It will include details regarding what will be shared, when, why and what the legal justification for disclosure is.

Where the request is to be reviewed and signed by specific individuals for example the Caldicott Guardian; it is the organisations position that it will be the responsibility of the Service Manager disclosing or receiving the information to review and sign. The Service manager will be supported by the Information Governance Team and the Caldicott Guardian if required.

Additional guidance will be provided to ensure any agreements contain suitable information and controls.

### 11.3. Methods of Information exchange/sharing

Once and appropriate basis for sharing information has been identified, a secure method should be chosen that complies with this and other relevant policies. Key messages should be considered below:

#### Sharing Information by Phone

Staff member must:

- Confirm the name, job title, department and organisation of the person requesting the information;
- Confirm the reason for information request if appropriate;
- Take a contact telephone number, for example, the main switchboard number;
- Check whether the information can be provided. If in doubt, tell the enquirer you will call them back;
- Provide the information only to the person who has requested it. Do not for example leave such information in the form of a message; and
- Ensure that you record your name, date and the time of disclosure, the reason for it and who authorised it. Also record the recipient's name, job title, organisation and telephone number.

## Sharing PCD Information by Post

When sharing information by post, the staff member must:

- Confirm the name, department and address of the recipient;
- Seal the information in a robust envelope;
- Mark the envelope 'Private & Confidential – to be opened by Addressee only';
- When appropriate, send the information by Recorded Delivery; and
- When necessary, ask the recipient to confirm receipt.

## Transporting Information

Information must be secure at all times and not left visible to others.

## Sharing PCD Information by Fax

The CCG will make available guidance on how to securely exchange information however will specifically discourage the use of faxes to transfer information unless absolutely necessary and must.

- Telephone the recipient of the fax to let them know they are going to send information;
- Ask them to acknowledge receipt of the fax;
- Double check the fax number; (test if it's not been used before)
- Use a fax cover sheet states who the information is for, and mark it 'Private & Confidential'; and
- Ask the recipient to confirm safe receipt
- If appropriate, request a report sheet to confirm that transmission was OK.

## 12. Training requirements

Information Security is fundamental in everyone's training, and therefore will form part of mandatory training. This will be reviewed and documented within the IG training needs analysis and delivery plan, to ensure it meets the relevant job roles within this policy.

## 13. Relationship with Service Providers

As a commissioner of clinical and support services the CCG will ensure that any organisations from which buy's services from meets expected information governance standards.

### 13.1. Clinical Services

All clinical services commissioned by or on behalf of the CCG will be required to:

- Have a suitable contract in place to form a joint data controller relationship in relation to the information required to effectively monitor commissioned services
- Ensure the services commissioned meet the requirements of the Data Protection Act when providing services including, but not limited to fair processing, maintaining a registration with the [Information Commissioners Office](#)
- Complete the annual [Information Governance Toolkit](#) and undertake an independent audit to be disclosed to the CCG on request in order to provide assurance they have met expected requirements.
- Ensure privacy notices make individuals aware of a CCGs role in commissioning and the personal and sensitive data it may receive to undertake such a role
- Ensure that where any IG incidents occur that they are reported to the CCG via routes determined within the contract
- Ensure the contract stipulates sufficient security controls to meet or exceed requirements set out in this policy.

## 13.2. Support services

All support services that process information on behalf of the CCG will be required to ensure:

- The contract stipulates sufficient security controls to meet or exceed requirements set out in this policy. This should be in the relevant standard NHS contract.
- A suitable contract is in place to form a Data Controller to Data Processor relationship where Personal or Personal Sensitive data is managed on behalf of the CCG.
- Ensure the services commissioned meet the requirements of the Data Protection Act when providing services including, but not limited to, fair processing and maintaining a registration with the [Information Commissioners Office](#)
- Completion of the annual [Information Governance Toolkit](#) and undertake an independent audit to be disclosed to the CCG on request to provide assurance they have met expected requirements.
- That any new processing is within the remit of the contract or seek written confirmation if there is any ambiguity
- Report any known incidents or risks in relation to the use or management of information owned by the CCG

## 14. Equality and Diversity

As part of its development, this policy and its impact on staff, patients and the public have been reviewed in line with expected 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 protected characteristics such as race, social exclusion, gender, disability, age, sexual orientation or religion/belief.

The equality impact assessment has been completed and has identified impact or potential impact as “minimal impact”.

## 15. Dissemination and Implementation

This policy will be made available to all relevant stakeholders via the CCG internet site. Additionally they will be made aware via email and this policy will be included for reference where necessary.

The policy will be supported by additional related policies and resources to support implementation. This will include the availability of, and access to, written and verbal advice, guidance and procedures where necessary.

## 16. Non-conformance with this Policy

Should it not possible to meet the requirements within this policy and associated guidelines this must be brought to the attention of the department's Information Asset Owner. Any issues will need to be documented as a risk and either:

- a. Accepted and reviewed in line with this policy
- b. Accepted with a view to implementing an action plan to reduce the risk
- c. Not accepted and the practice will stop until such time as the risk can be reduced

Failure to comply with the standards and appropriate governance of information as detailed in this policy, supporting protocols and procedures can result in disciplinary action. All staff are reminded that this policy covers several aspects of legal compliance that as individuals they are responsible for. Failure to maintain these standards can result in criminal proceedings against the individual. These include but are not limited to:

- Common law duty of confidentiality
- Computer Misuse Act 1990
- Data Protection Act 1998
- Freedom of Information Act 2000
- Human Rights Act 1998
- Public Records Act 1958
- Health & Social Care Act 2012

## **17. Monitoring and Review**

Performance against the policy will be monitored against

- Availability and dissemination of policy, including in alternative formats where requested or need identified
- Acceptance and understanding of audience (training, spot checks, surveys)
- Reports of non-conformance i.e. incidents or risks
- Compliance against the Information Governance Toolkit

This policy will be reviewed every 2 years and in accordance with the following on an as and when required basis:

- Legislative or case law changes;
- changes or release of good practice or statutory guidance;
- identified deficiencies, risks or following significant incidents reported;
- changes to organisational infrastructure.

### **17.1. Monitoring of individuals**

In order to ensure compliance with the Law, organisational policies; including this one, the CCG reserves the right to monitor usage and content where it suspects that there has been a breach of policy. The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- In the interests of national security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system.

In addition, communications may be monitored (but not recorded) for the purpose of checking whether those communications are relevant to the purpose of the CCG's business, and the employee's position with the CCG. Any monitoring will be undertaken in accordance with the above act and the Human Rights Act.

This will include the use or access to any Network or where the property of the Organisation is used in the communication or is accessed remotely from outside the Organisation. This includes the use of portable computers and mobile devices, including mobile phones issued to the employee by the Organisation.

### **18.1 Compliance Standards**

- Common law duty of confidentiality
- Computer Misuse Act 1990
- Data Protection Act 1998
- Freedom of Information Act 2000
- Human Rights Act 1998
- Public Records Act 1958

## Appendices

### Appendix A. Evaluation protocol

Monitoring requirements 'What in this document do we have to monitor'	<p>The management of information risks (Information Risk Management)</p> <p>Compliance with the law</p> <p>Compliance with the Information Governance Toolkit</p> <p>Incidents related to the breach of this policy</p> <p>Destruction of Information Assets</p> <p>Registration of Data Flows and Information Assets</p> <p>Compliance with Registration Authority Terms and Conditions</p> <p>Network Penetration testing</p> <p>Monitoring of inappropriate access to systems (where possible)</p>
Monitoring Method	<p>Information Risks will be monitored through the Risk Register and management system.</p> <p>Compliance with law will be monitored through audit, work directed by the Information Governance Toolkit and as directed by the SIRO</p> <p>The Information Governance Toolkit will be monitored by assessment of evidence against the objective of the relevant requirement. In addition, the IGT will be audited by the organisation's internal audit function before the annual submission.</p> <p>Incident reporting and management requirements</p>
Monitoring prepared by	<p>The CSU Information Governance Team and the CCG IG Lead for the relevant groups</p> <p>Incident reports will be produced by the nominated investigation officer</p>
Monitoring presented to	<p>Relevant CCG committees or groups with oversight of Information Governance</p> <p>Senior Information Risk Owner</p> <p>Caldicott Guardian</p>
Frequency of Review	<p>Yearly updates will be provided to the relevant groups, the SIRO and the CG</p> <p>Relevant Information Risks will be added to the Corporate Risk Register and reported in line with Risk Management system</p> <p>Annual (as a minimum) updates to the Board will be provided. The internal audit report on IGT performance will be provided to the Board or delegated sub-committee.</p> <p>Incident Reports will be reviewed on an annual basis and as directed by the seriousness of the incident</p>

## Appendix B. Equality and Equity Impact Assessment

This is a checklist to ensure relevant equality and equity aspects of proposals have been addressed either in the main body of the document or in a separate equality & equity impact assessment (EEIA)/ equality analysis. It is not a substitute for an EEIA which is required unless it can be shown that a proposal has no capacity to influence equality. The checklist is to enable the policy lead and the relevant committee to see whether an EEIA is required and to give assurance that the proposals will be legal, fair and equitable.

The word proposal is a generic term for any policy, procedure or strategy that requires assessment.

	Challenge questions	Yes/ No	What positive or negative impact do you assess there may be?
1.	Does the proposal affect one group more or less favourably than another on the basis of:	No	
	▪ Race		
	▪ Ethnic origin (including gypsies and travellers, refugees & asylum seekers)		
	▪ Nationality		
	▪ Gender		
	▪ Culture		
	▪ Religion or belief		
	▪ Sexual orientation (including lesbian, gay bisexual and transgender people)		
	▪ Age		
	▪ Disability (including learning disabilities, physical disability, sensory impairment and mental health problems)		
2.	Will the proposal have an impact on lifestyle? (e.g. diet and nutrition, exercise, physical activity, substance use, risk taking behaviour, education and learning)	No	
3.	Will the proposal have an impact on social environment? (e.g. social status, employment (whether paid or not), social/family support, stress, income)	No	
4.	Will the proposal have an impact on physical environment? (e.g. living conditions, working conditions, pollution or climate change, accidental injury, public safety, transmission of infectious disease)	No	
5.	Will the proposal affect access to or experience of services? (e.g. Health Care, Transport, Social Services, Housing Services, Education)	No	

An answer of 'Yes' to any of the above question will require the Policy lead to undertake a full Equality & Equity Impact Assessment (EEIA) and to submit the assessment for review when the policy is being approved.

## Appendix C. Definitions

Term	Definition	Source
Data	Data is used to describe 'qualitative or quantitative statements or numbers that are assumed to be factual, and not the product of analysis or interpretation.'	Definition taken from The Information Governance Review, Mar 2013 (Gateway Ref: 2900774) <sup>1</sup> based on the Cabinet Office definition
Information	Information is the 'output of some process that summarises interprets or otherwise represents data to convey meaning.'	Definition taken from The Information Governance Review, Mar 2013 (Gateway Ref: 2900774)
Personal Confidential Data or PCD	This term describes personal information about identified or identifiable individuals, which should be kept private or secret. For the purposes of this review 'personal' includes the Data Protection Act definition of personal data, but it is adapted to include dead as well as living people and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence' and is adapted to include 'sensitive' as defined in the Data Protection Act.	Definition taken from The Information Governance Review, Mar 2013 (Gateway Ref: 2900774)

<sup>1</sup> See [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/192572/2900774\\_InfoGovernance\\_accv2.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf),  
Waltham Forest CCG Confidentiality and Disclosure of Information Policy October 2015 Page 20 of 24

# Confidentiality and Information Sharing

## Quick Reference Guide

This summary is intended to be a helpful reminder for all employees. It is not intended to be a comprehensive list of user responsibilities and does not reduce or alter the standards or principles in the Confidentiality and Information Sharing Policy.

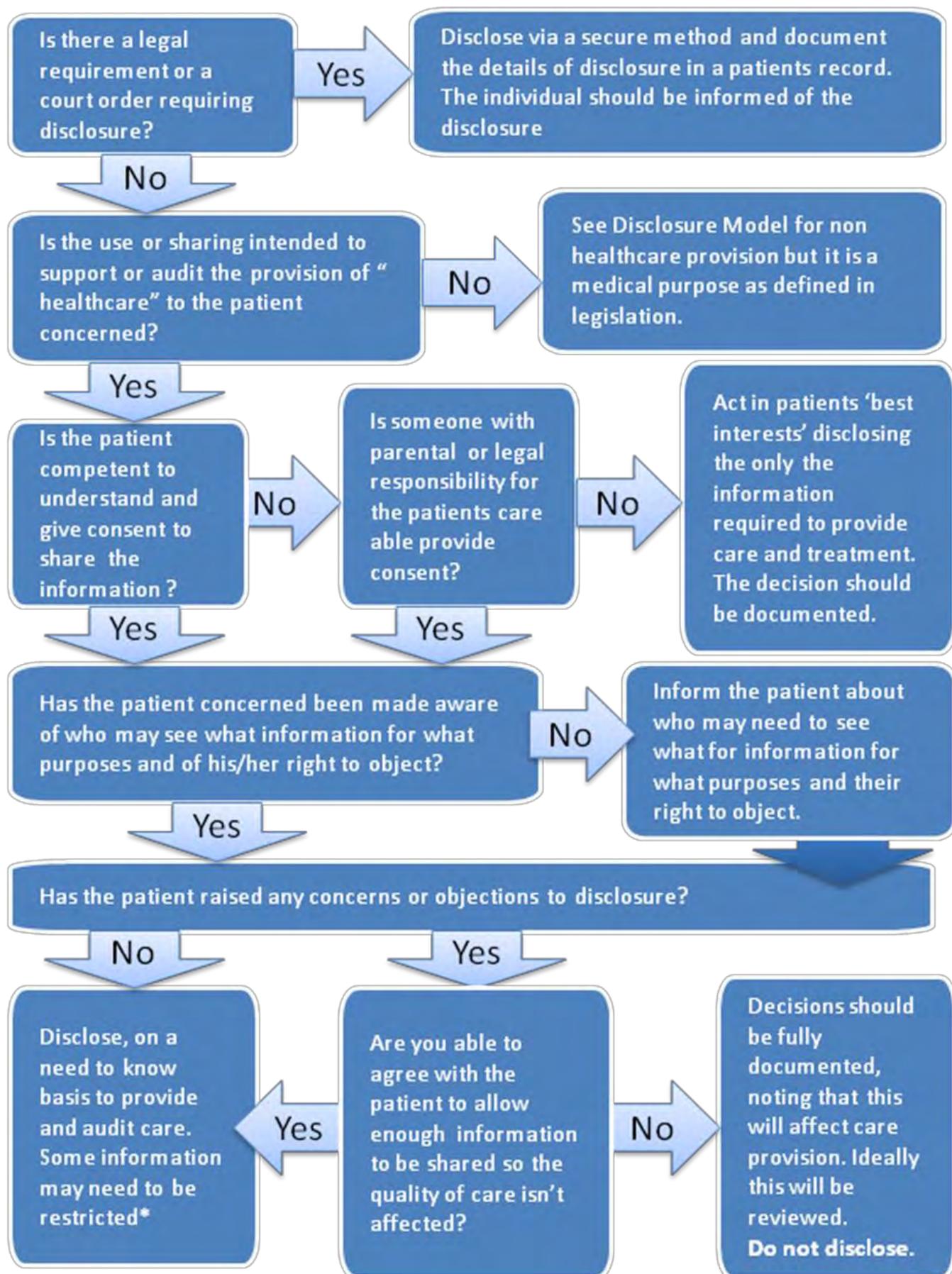
### All Staff should:

#### Understand what is

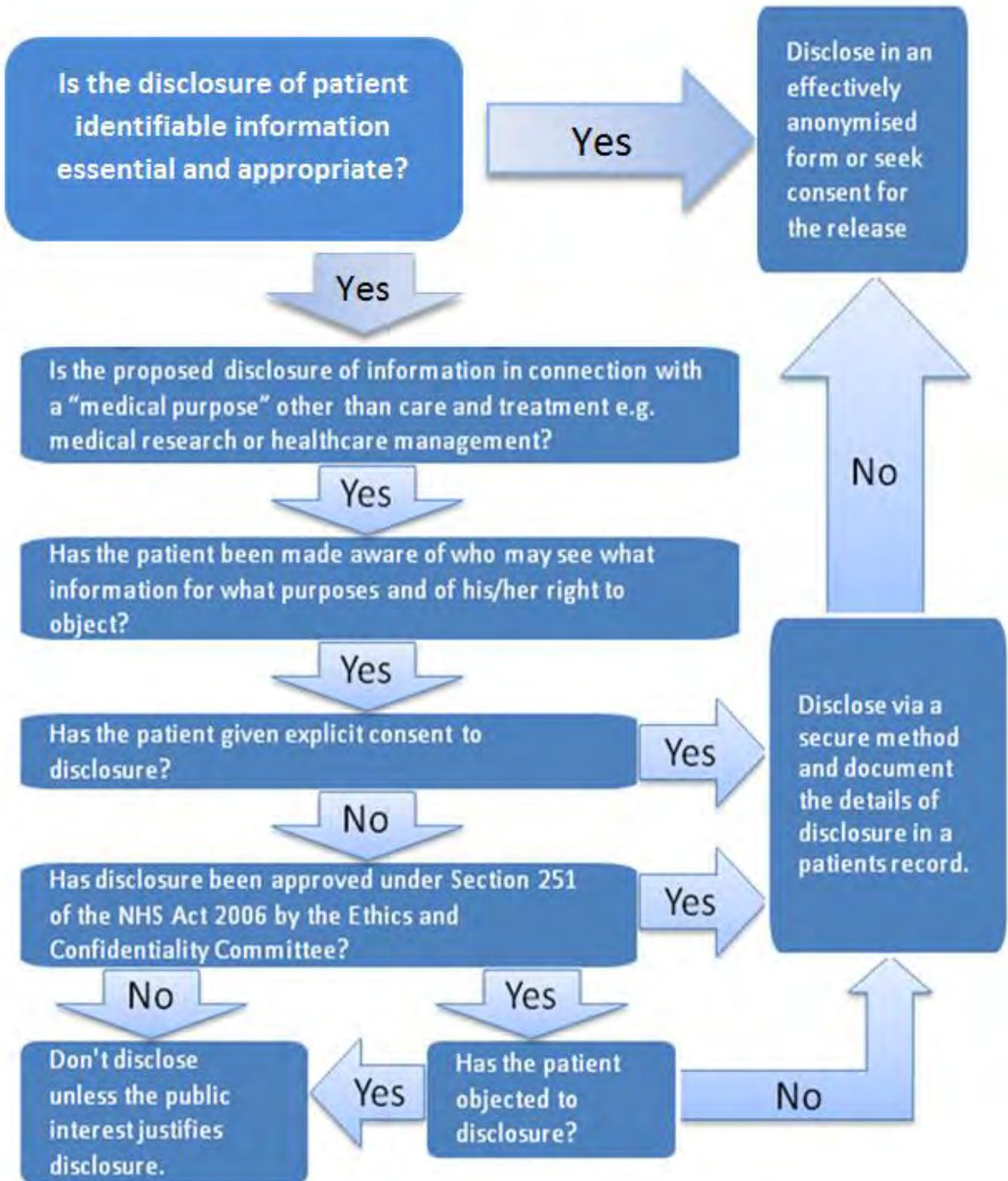
1. NHS Official- Sensitive; NHS Official- Sensitive: Commercial NHS Official- Sensitive: Personal marked information
1. Treat NHS Official- Sensitive; NHS Official- Sensitive: Commercial NHS Official- Sensitive: Personal information in the strictest of confidence.
2. Store all NHS Official- Sensitive; Commercial: Personal securely to prevent unauthorised access,
  - a. Manual (Paper information) should, for example, be locked away when unattended
  - b. Electronic information should be in systems with restricted access (Based upon user rights)
  - c. Information on portable media/devices must be encrypted.
  - d. and destroy all out of date information securely
3. Unless justified and for the healthcare only use or disclose information that wouldn't identify the individual. I.e. anonymised/pseudonymised information.
4. Only give information to those individuals who need-to-know that information, and have a legitimate right to receive it.
5. Ensure that all information received from, or sent to, another individual is secure in transit, whether the information is sent manually or electronically.
6. Maintain secrecy of computer passwords and security codes to locked areas.
7. Always log off or lock your information away before leaving your desk. (Computers or cupboards)
8. Be vigilant of where conversations take place to prevent unintentional disclosure of information through overheard conversations.
9. Never give person identifiable information over the telephone to an incoming caller without confirming the identity of caller and legitimacy of request.
10. Ensure you are aware of current local and national policies and procedures relevant to your job role.

For further information, please contact the [Information Governance Team](#).

**Appendix E. Disclosure Model where it is proposed to share confidential information in order to provide healthcare.**



Appendix F. Disclosures for non-healthcare provision but a medical purpose in legislation.



Disclosures unrelated to healthcare or another medical purpose.

