

# **Confidentiality and sharing information policy**

## **Ref CORP-0010-v10**

**Status: Ratified**

**Document type: Policy**

## Contents

<b>1</b>	<b>Introduction.....</b>	<b>3</b>
<b>2</b>	<b>Why we need this policy .....</b>	<b>3</b>
2.1	Purpose .....	4
2.2	Objectives.....	4
<b>3</b>	<b>Scope.....</b>	<b>5</b>
3.1	Who this policy applies to .....	5
3.2	Roles and responsibilities .....	5
<b>4</b>	<b>Policy.....</b>	<b>6</b>
4.1	The legislative framework .....	6
4.2	Defining confidentiality .....	7
4.3	Right of access .....	7
4.4	Confidentiality and Caldicott .....	7
4.5	Information sharing principles .....	8
4.5.1	Information Sharing Agreements .....	8
<b>5</b>	<b>Single point of contact .....</b>	<b>8</b>
<b>6</b>	<b>Sharing information with carers and/or family members.....</b>	<b>9</b>
<b>7</b>	<b>Recording disclosures .....</b>	<b>9</b>
<b>8</b>	<b>Breaching confidentiality .....</b>	<b>9</b>
<b>9</b>	<b>Definitions .....</b>	<b>10</b>
<b>10</b>	<b>Related documents.....</b>	<b>11</b>
<b>11</b>	<b>How this policy will be implemented.....</b>	<b>11</b>
<b>12</b>	<b>How this policy will be audited .....</b>	<b>11</b>
<b>13</b>	<b>References .....</b>	<b>11</b>
<b>14</b>	<b>Appendices .....</b>	<b>12</b>
14.1	Appendix 1: Determining confidentiality - decision support tree .....	12
14.2	Appendix 2: NHS Digital (HSCIC) Confidentiality Rules .....	13
14.3	Appendix 3: NHS Digital's (HSCIC) Seven golden rules .....	18
<b>15</b>	<b>Document control .....</b>	<b>19</b>

---

## 1 Introduction

---

*“Multi-agency working, collaboration and partnership are central to government philosophy of ensuring everyone involved in improving the health of individuals and their families plays their part”.*

**(Secretary of State for Health, 1999, pp. 1.31-1.40)**

Government policy puts patients and their families at the centre of care planning with agencies working together around them to deliver care. Meanwhile, professionals are bound by legislation and codes of practice to maintain confidentiality of patient information.

The Trust’s mission is to put the service user at the centre of everything that we do and confidentiality and information sharing is no different in this respect. There can be grey areas and this policy will help you in those cases. An understanding of the individual needs of service users should always be at the centre of decisions that are made. The seventh Caldicott Principle reinforces the fact that sometimes information must be shared and confidentiality breached if it is in the best interests of a service user or in the public interest.

There are occasions when a carer asks for help so that they can support the service user that they are working with. It does not breach confidentiality to help carers to understand more about a condition and how they can help the service user achieve and maintain their recovery. It is already well understood that the work of a carer in support of a service user’s recovery is essential and an integral part of the care package.

Staff must understand when to share information with other professionals, and when not to share, so they can provide the best standard of care.



Lives may be lost if information is not shared as it should be.

The 7th Caldicott principle recognises this when it states *‘the duty to share information can be as important as the duty to protect confidentiality’*.

Adhering to this policy will ensure we use information in a lawful way. It aims to help practitioners balance the contradiction between their obligations to preserve patient confidentiality and the need for information to be shared to provide the best care for our service users.’

---

## 2 Why we need this policy

---

The Health and Social Care Information Centre (HSCIC)’s Guide to Confidentiality in Health and Social Care (Rule 5) says that we should put policies, procedures and systems in place to ensure confidentiality rules are followed.

The Health and Social Care (Safety and Quality) Act 2015 introduced a new legal duty requiring health and adult social care bodies to share information where this will facilitate care for an individual. This new legislation requires and provides a clear message that subject to the preferences of the individuals concerned, sharing for the care of individuals is a requirement, not an option.

The new data protection laws (General Data Protection regulation 2016 and UK Data Protection Act 2018) still recognise the importance of the common law duty of confidentiality.

Information is considered to be confidential when it meets these criteria:

- The information must have the necessary quality of confidence;
- The information must be imparted in circumstances giving rise to an obligation of confidence, e.g. a service user disclosing health information about themselves to a doctor or nurse

A breach in confidence is actionable when there is unauthorised use of that information to the detriment of the original communicator of the information.

## 2.1 Purpose

---

This policy describes how personal confidential information should be protected or shared to:

- ensure service users trust the organisation to respect their information;
- ensure all staff understand when they must share information and when they should not;
- provide the best quality healthcare by ensuring service users trust us enough to disclose personal confidential information;
- ensure lives are not lost if information is not shared when it should be;
- ensure we do not surprise service users with how we use their information.

## 2.2 Objectives

---

Adhering to this policy will ensure:

- Confidential information is used lawfully;
- The organisation earns trust and respect from our service users;
- Staff keep information confidential whilst at the same time not compromising the requirement to share information where appropriate;
- Our service users have the opportunity to tell us who they do not want their information shared with;
- The Trust complies with the recommendations set out in the NHS Constitution, Care Record Guarantee and Caldicott sorted.

## 3 Scope

This policy focuses on service user confidentiality, but all staff must understand that staff information must also be handled with regard to confidentiality. Although the Caldicott Principles detailed in section 4 relates specifically to patient identifiable information, they can just as easily be applied to staff identifiable information.

### 3.1 Who this policy applies to

This policy applies to all staff, students, volunteers and contractors.

### 3.2 Roles and responsibilities

Role	Responsibility
Chief Executive	<ul style="list-style-type: none"> <li>Ultimate responsibility for all aspects of how information is collected, stored and used by the Trust to maintain confidentiality.</li> </ul>
Caldicott Guardian and deputy Caldicott Guardian	<ul style="list-style-type: none"> <li>Ensuring the organisation continues to meet its requirements as set out in the Health and Social Care Information Centre (HSCIC)'s Guide to Confidentiality in Health and Social Care</li> <li>Protecting the confidentiality of patient and service-user information and enabling appropriate information sharing. They act as the conscience of the organisation, ensuring that both legal and ethical considerations are taken into account, particularly when deciding whether to share confidential information. It is their job to embed a culture of confidentiality within the organisation.</li> <li>The Trust's Caldicott Guardian is the Director of Nursing and Governance, and the Deputy Caldicott Guardian is the Deputy Director of Nursing.</li> </ul>
Data Protection Officer	<ul style="list-style-type: none"> <li>The Trust's Data Protection Officer is the Head of Information Governance. The Data Protection Officer upholds the General Data Protection Regulation 2016 and Data Protection Act 2018.</li> </ul>
Managers and supervisors	<ul style="list-style-type: none"> <li>Ensuring that new staff understand the need for confidentiality through local induction. They must discuss confidentiality and how it applies to the individual's role. This must be recorded on the local induction checklist.</li> </ul>
Information Security Officer	<ul style="list-style-type: none"> <li>Facilitate the completion of Data Protection Impact Assessments (DPIAs) to assess the impact on an individual's privacy of using information and what control measures are necessary and proportionate. This individual also maintains a</li> </ul>

	public log of completed DPIAs.
Privacy Officer	<ul style="list-style-type: none"> <li>Monitoring potential privacy breaches through the PARIS Break Glass function and monitors actual privacy breaches through the Close Monitoring procedure.</li> </ul>
All staff, students, volunteers and contractors	<ul style="list-style-type: none"> <li>Maintaining and protecting the confidentiality of patient information which they use in their day to day roles.</li> <li>Maintaining confidentiality of staff and business information.</li> </ul>

## 4 Policy

---

### 4.1 The legislative framework

---

There are laws to ensure we protect both service users and staff when using personal confidential information:

- Common Law of Confidentiality
- Data Protection Act 2018 (DPA)
- General Data Protection Regulation 2016 (GDPR)
- Human Rights Act 1998
- Mental Health Act 1983: Code of Practice
- Access to Health Records Act 1990 (protects the health information of deceased individuals)

These are supported by the Caldicott principles (see section 4.4) to help us think how we provide quality and safe patient care whilst preserving a patient's rights to confidentiality.

Data Protection laws changed on the 25<sup>th</sup> May 2018 with the implementation of the GDPR and DPA. Going forwards the Trust will not rely on consent as the legal basis for processing personal information for the delivery of direct care. We will be relying on Article 6(1)(c) and Article 9(2)(h) of the GDPR.

Article 6(1)(c):

*Processing is necessary for compliance with a legal obligation to which the controller is subject.*

The Trust has to comply with a number of legal obligations such as the Health and Social Care Act 2012 and Mental Health Act 1983.

Article 9(2)(h)

*Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, **the provision of health or social care or treatment or the management of health or social care systems and services.***

The Trust relies on this article because it is using health information to deliver the correct treatment for individuals. Health information (physical and mental) is classed as a 'special category' of

information in data protection law. It was formerly known as ‘sensitive’ information under the former data protection law (Data Protection Act 1998).

What this means is that when it is necessary to share personal information for the delivery of direct health care consent is not needed. However, an individual needs to know how the Trust intends to use their personal information. Clinical staff must discuss the use of personal information with service users. The Trust’s Privacy Notice will help service users understand how we use their personal information. It is a legal duty to provide service users with a Privacy Notice. This is published on TEWV’s internet site.

## 4.2 Defining confidentiality

It is important to be clear about what is confidential - and what isn’t. It is part of our role to help carers and families understand the type of illness their loved one is struggling with, particularly if they are asking for your help.

Consider also the ‘*obligation of confidentiality*’ – were we given the information on the understanding that it would be kept confidential?

For example, sharing information with a carer about the common symptoms and behaviours associated with depression and the help and support that is available to them is **not** the same as sharing information about a service user’s individual symptoms.

Refer to Appendix 1 for a decision tree to help you decide if information is confidential.

## 4.3 Right of access

Under the Data Protection Act 2018, the Trust has a responsibility to collect, record and use special categories of personal information in its role as a Data Controller. This Act also gives all data subjects (the person the information is about) the right to access information held about them. (Refer to the Trust’s Requests for Information Procedure).

## 4.4 Confidentiality and Caldicott



Staff must follow the Caldicott Principles when sharing confidential patient information.

Principle		Question
1	Justify the purpose	Do we have a really good reason for sharing this?
2	Do not use patient identifiable information unless it is absolutely necessary	Could we share this without identifying the service user?
3	Use the minimum necessary patient identifiable information	What is the least information we can share? Do the receivers need to know all of this?

<b>4</b>	Access to patient identifiable information should be on a strict need-to-know basis	Do I need to know this? Do the receivers need to know this?
<b>5</b>	Everyone should be aware of their responsibilities	Do I understand this policy and other published literature on confidentiality including the HSCIC's ' <a href="#">A Guide to Confidentiality in Health &amp; Social Care</a> ', ' <a href="#">Confidentiality: NHS Code of Practice</a> ' and the Information Governance Alliance's ' <a href="#">Duty to Share Information</a> '?
<b>6</b>	Understand and comply with the law	Does what I'm sharing comply with the common law duty of confidentiality, data protection law (GDPR and DPA) and Human Rights Act 1998?
<b>7</b>	The duty to share information can be as important as the duty to protect patient confidentiality.	Am I sharing this information in the best interests of the individual?

## 4.5 Information sharing principles

There are two main types of information shared within and outside of the Trust:

- **Systematic** – routine data sharing for an established purpose - this should be managed by an information sharing agreement (see 4.5.1 below)
- **Exceptional** – one-off decisions to share data for any of a range of purposes. Caldicott principles apply and approval may be required from the Caldicott Guardian. You can also refer to the NHS Digital rules at Appendix 2 and NHS Digital's seven golden rules at Appendix 3 to help you determine whether information should or not should be shared.

### 4.5.1 Information Sharing Agreements


When information that can identify an individual is shared, both the disclosing and receiving organisations should have procedures that:

- meet the requirements of law and guidance, and
- make clear to staff the proper working practices.

These procedures (and the law and guidance on which they are based) are often set out within an information sharing agreement or protocol.

A register of the Trust's information sharing agreements (ISAs) is maintained by the Information Governance Department. ISAs are published on the [trustwide shared drive](#). If you need to establish an information sharing agreement, please contact the Head of Information Governance.

## 5 Single point of contact



In circumstances where special categories (sensitive) information needs to be shared with our Trust but no contact is known, the Trust's confidential Single Point of Contact (SPOC) is:

**Elizabeth Moody**



**Caldicott Guardian / Director of Nursing and Governance**  
**Tarncroft**  
**Lanchester Road Hospital**  
**Lanchester Road**  
**Durham**  
**DH1 5RD**  
**Safe Haven Fax 01642 516491**  
**Telephone: 0191 333 6633**  
**Email: [tewv.archiverequests@nhs.net](mailto:tewv.archiverequests@nhs.net)**

## **6 Sharing information with carers and/or family members**

---

It is almost always important to help carers and families to understand the type of illness with which their loved one is struggling, particularly if they are asking for your help. This does not mean that you are sharing information about the patient's individual symptoms. An example of this might be if you have a patient with depression, it is perfectly appropriate to have a conversation with the carer about the common symptoms and behaviours associated with depression and the help and support that is available to both the patient and the carer.

The Trust will support the sharing of appropriate information with third parties such as carers and/or family members if you feel it is essential to safeguard the individual concerned. Supporting a staff member who has breached confidentiality to save a person's life will always be preferable to explaining why information has been withheld that could have made a difference.

## **7 Recording disclosures**

---

Any decision to disclose confidential information about patients – for any reason – should be fully documented. The relevant facts should be recorded, along with the reasons for the decision and the identity of all those involved in the decision-making. Reasons should be given by reference to the grounds on which the disclosure is to be justified. (MHA 1983: Code of Practice para.10.18)

## **8 Breaching confidentiality**

---

All breaches of confidentiality will be investigated by the Trust.

If staff, students, volunteers and contractors intentionally and maliciously breach confidentiality, these incidents will be investigated and individuals may be subject to disciplinary action including dismissal.

Some incidents may be so serious that perpetrators will be taken to court and fined and other sanctions imposed.

## 9 Definitions

Term	Definition
Common law duty of confidentiality	<p>This is not legislated by an Act of Parliament but built up from case law where practice has been established by individual judgements. The key principle is that information confided should not be used or disclosed further, except as originally understood by the confider, or with their subsequent permission.</p> <p>Whilst judgements have established that confidentiality can be breached 'in the public interest', these have centred on case-by-case consideration of exceptional circumstances. Confidentiality can also be overridden or set aside by legislation.</p>
Consent	<p>The approval or agreement for something to happen after consideration.</p> <p>For consent to be legally valid, the individual must be informed, must have the capacity to make the decision in question and must give consent voluntarily. This means individuals should know and understand how their information is to be used and shared (there should be '<i>no surprises</i>') and they should understand the implications of their decision, particularly where refusing to allow information to be shared is likely to affect the care they receive. This applies to both explicit and implied consent.</p> <p>Silence, pre-ticked boxes or inactivity does not constitute consent. Consent may be withdrawn at any stage and this must be recorded in the patient record. Data subjects must be told they have a right to withdraw consent. (Refer to the Trust's Privacy Notice published on the Trust's internet).</p>
Data controller	<p>A person or organisation who determines the purposes for which and the manner in which any personal data are, or are to be processed (see Data Protection Act 2018).</p>
Direct care	<p>A clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. It includes supporting individuals' ability to function and improve their participation in life and society. It includes the assurance of safe and high quality care and treatment through local audit, the management of untoward or adverse incidents, person satisfaction including measurement of outcomes undertaken by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship for their care.</p>
Duty of confidence	<p>Arises when one person discloses information to another (e.g. patient to clinician) in circumstances where it is reasonable to expect that the information will be held in confidence.</p>
HSCIC	<p>Health and Social Care Information Centre – now called NHS Digital. NHS Digital is the national provider of information, data and IT systems for commissioners, analysts and clinicians in health and social care.</p>

## 10 Related documents

---

Communicating with service users procedure (not yet available)

[Induction policy](#)

[Information Governance Policy](#)

[Information Security and Risk Policy](#)

[Records Management Policy](#)

[Mental Capacity Act Policy](#)

[Trust Privacy Notice](#)

[Monitoring and Auditing Service User Confidentiality Procedure](#)

[Incident Reporting and Serious Incident Review Policy](#)

[Minimum standards for clinical record keeping](#)

[Minimum standards for corporate record keeping](#)

## 11 How this policy will be implemented

---

- This policy will be published on the Trust's intranet and external website.
- Line managers will disseminate this policy to all Trust employees through local induction.
- The subject of confidentiality will be covered in annual information governance mandatory training.
- A requirement of this policy is that staff read the HSCIC's 'A Guide to Confidentiality in Health and Social Care'.

## 12 How this policy will be audited

---

- Confidentiality and privacy will be monitored through the Paris Break Glass function and through the Close Monitoring procedure by the Trust's Privacy Officer.

## 13 References

---

[HSCIC Guide to Confidentiality in Health and Social Care 2013](#)

[HSCIC Code of Practice on Confidential Information 2014](#)

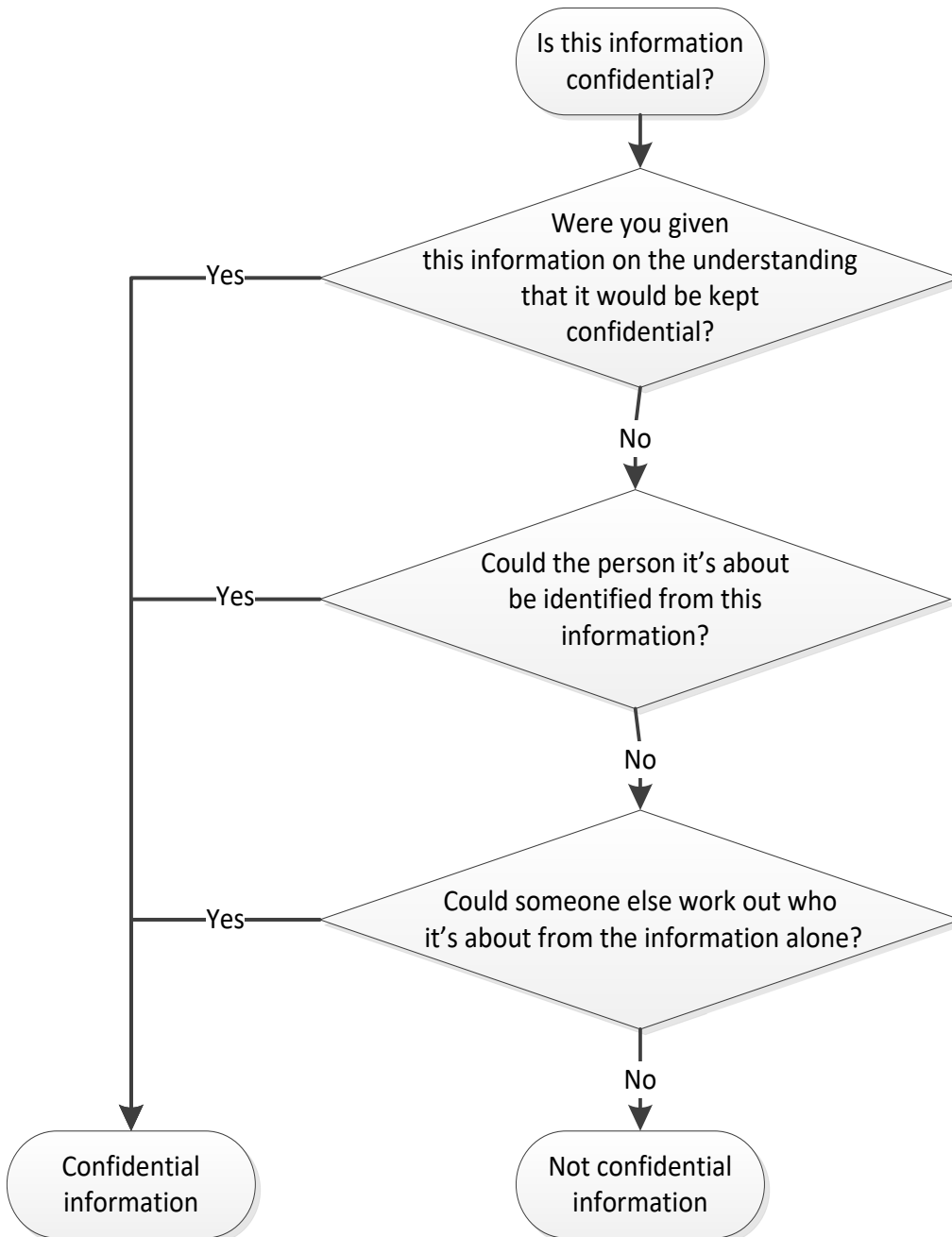
[Confidentiality: NHS Code of Practice, Supplementary Guidance on Public Interest Disclosures](#)

[Information Security Management: NHS Code of Practice](#)

[NHS Digital Information Sharing Resources](#)

## 14 Appendices

### 14.1 Appendix 1: Determining confidentiality - decision support tree



Based on HSCIC Code of Practice on confidential information Dec 2014 P 29

## 14.2 Appendix 2: NHS Digital (HSCIC) Confidentiality Rules

The Health and Social Care Information Centre (HSCIC) has established five confidentiality rules that people are entitled to expect to be followed in care settings run by the NHS or publicly funded adult social care services.

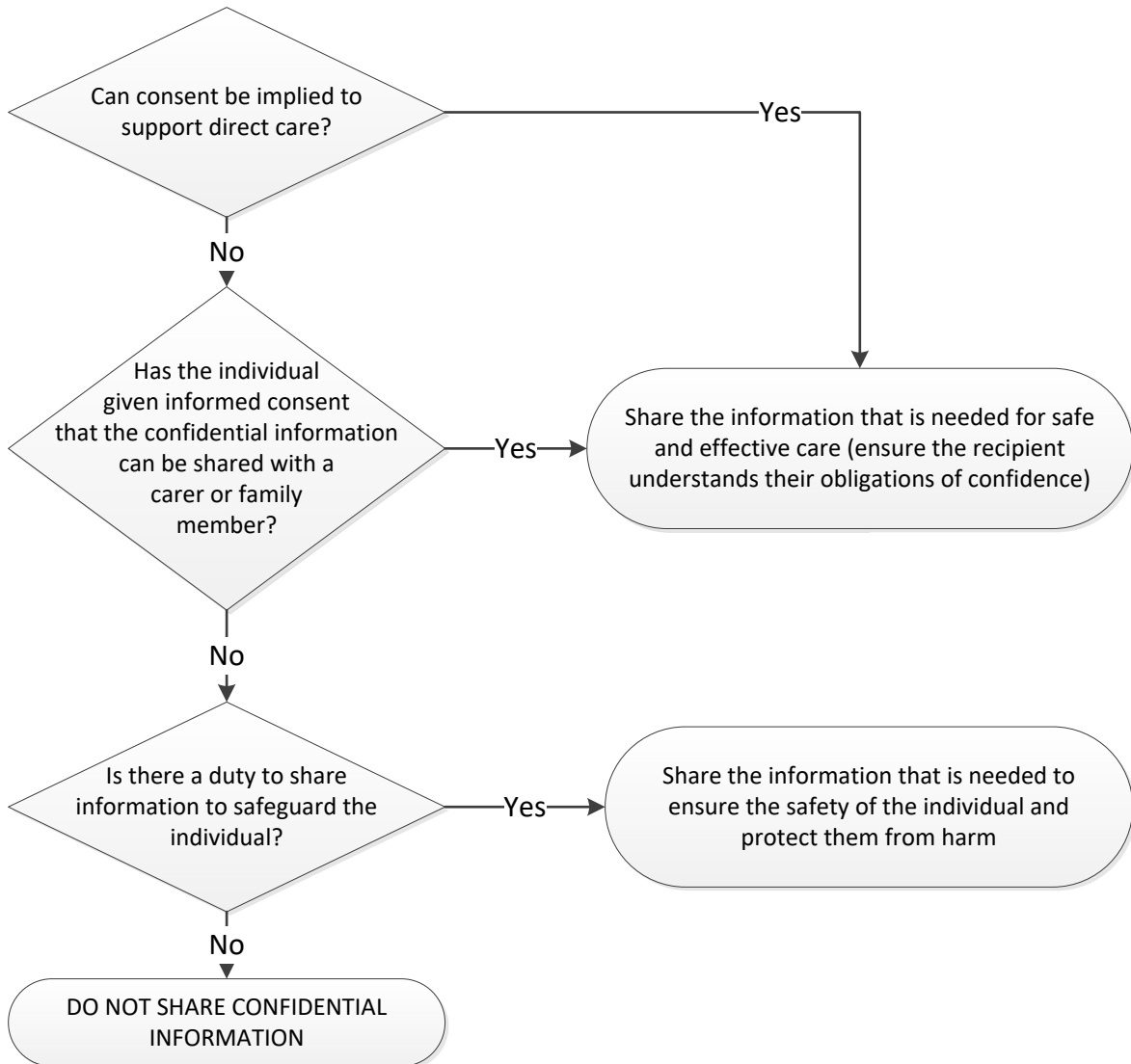
### Rule 1 - Confidential information about service users or patients should be treated confidentially and respectfully

- No prying or gossiping – it's unethical in all settings.
- Create an environment of trust which encourages people to be open and honest with those who care for them.
- Follow Trust policies and procedures when moving confidential information, incorporating safe haven principles where necessary.
- If confidential information about an individual is disclosed in error, we will explain and apologise – as long as disclosing a confidentiality breach would not harm an individual.
- Make sure staff and patient records are accurate and up-to-date.
- If you think confidentiality rules are not being followed, report it to the Trust's [Caldicott Guardian](#).
- If you believe there is a conflict of interest in any of the work you do in the Trust, for example, if someone you know outside of work is referred to your caseload, team or unit, discuss this with your line manager.

**Rule 2 - Members of a care team should share confidential information when it is needed for the safe and effective care of an individual**

**Implied consent** is the suggestion or indication from the individual that their information can be shared without the consent being directly or explicitly stated

Fig 1. Deciding whether to share confidential information for direct care



HSCIC Guide to Confidentiality in Health and Social Care 2013 p15

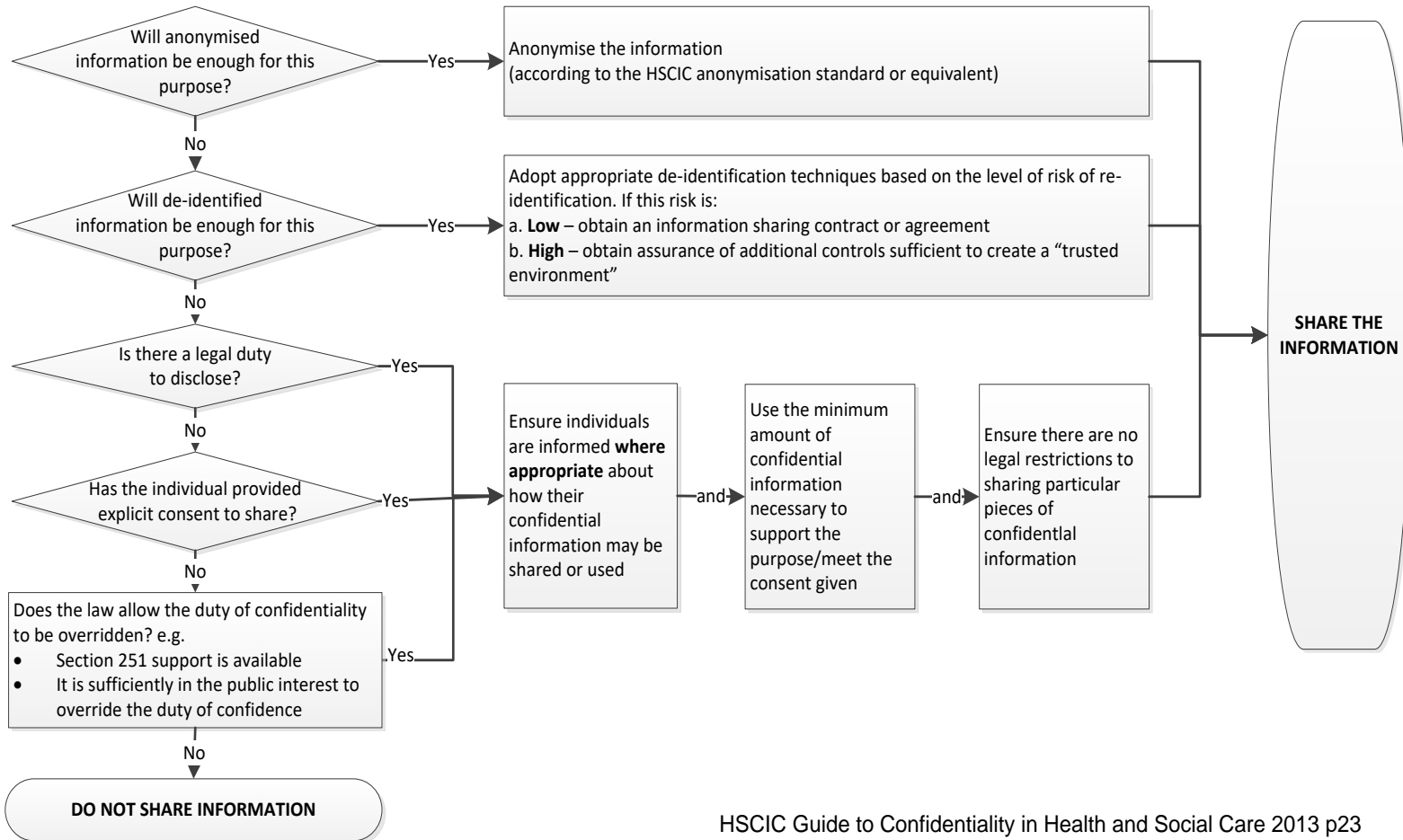
**Rule 3 - Information that is shared for the benefit of the community should be anonymised**

**Anonymised information** is in a form which does not identify individuals and where identification is not likely to take place. This allows for a much wider use of the information.

**De-identified information** is information that has had any details removed which could identify the original subject.

Sometimes we might want to share information about our service users or staff for the wider benefit of the community, such as for research. In its raw form, this information could be considered confidential, but if we can anonymise or de-identify the information, sharing may still be possible.

Based on Fig 2. Deciding whether to share or disclose confidential information for the benefit of the community



HSCIC Guide to Confidentiality in Health and Social Care 2013 p23



**Rule 4 - An individual's right to object to the sharing of confidential information about them should be respected**

- If an individual objects to particular items of confidential information being shared, we must usually respect that.
- Explain to the individual the risks of not sharing the information, so they can make an informed decision.
- Record any objections in the electronic patient record and give them a copy of the Trust's Privacy Notice.
- If the information you want to share can be anonymised, the individual's confidentiality wishes will still be respected.

**Rule 5 – Organisations should put policies, procedures and systems in place to ensure the confidentiality rules are followed.**

- See Section 6: Related Documents for details of supporting Trust policies and procedures

## 14.3 Appendix 3: NHS Digital's (HSCIC) Seven golden rules

Sometimes, it is difficult to know whether to share information or protect it. In this case, the HSCIS's Information sharing guidance gives clarity on when and how information can be shared legally, safely and professionally.

This guidance will be especially useful to support early intervention and preventative work where decisions about information sharing may be less clear than in safeguarding or child protection situations. The seven golden rules for information sharing are:

### Rule 1

Remember that the Data Protection Act is not a barrier to sharing information but provides a framework to ensure that personal information about living persons is shared appropriately.

### Rule 2

Be open and honest with the person (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.

### Rule 3

If you are in any doubt, seek advice, without disclosing the identity of the person where possible.

### Rule 4

Share with consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, that lack of consent can be overridden in the public interest. You will need to base your judgement on the facts of the case and the need to keep family or carers informed.

### Rule 5

Consider safety and well-being: Base your information sharing decisions on considerations of the safety and well-being of the person and others who may be affected by their actions.

### Rule 6

Is it:

- Necessary,
- proportionate,
- relevant,
- accurate,
- timely and
- secure?

Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those people who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely.

### Rule 7

Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

## 15 Document control

Date of approval:	13 June 2018	
Next review date:	13 June 2021	
This document replaces:	CORP-0010-v9.1 Confidentiality and Sharing Information Policy	
Lead:	Name	Title
	Louise Eastham	Head of Information Governance
Members of working party:	Name	Title
	Theresa Parks	Information Governance Manager
This document has been agreed and accepted by: (Director)	Name	Title
	Colin Martin	Director of Finance and Information
This document was approved by:	Name of committee/group	Date
	Digital Safety and Information Governance Board	10 May 2018
This document was ratified by:	Name of committee/group	Date
	Executive Management Team	13 June 2018
An equality analysis was completed on this document on:	March 2014	

### Change record

Version	Date	Amendment details	Status
9	04 Nov 2015		Withdrawn
9.1	01 Feb 2017	Section 4 - ref to MHA CoP added Section 6 added – recording disclosures	Withdrawn
10	May 2018	Data Protection Act 1998 changed to General Data Protection Regulation 2016 and Data Protection Act 2018.  Lawful basis for processing information described.	Ratified

## Equality Analysis Screening Form

**Please note; The Equality Analysis Policy and Equality Analysis Guidance can be found on InTouch on the policies page**

Name of Service area, Directorate/Department i.e. substance misuse, corporate, finance etc.	Information Governance			
Name of responsible person and job title	Theresa Parks – Information Governance Manager			
Name of working party, to include any other individuals, agencies or groups involved in this analysis	General Data Protection Regulation Steering Group			
Policy (document/service) name	Confidentiality and sharing information			
Is the area being assessed a...	Policy/Strategy	<input checked="" type="checkbox"/>	Service/Business plan	<input type="checkbox"/>
	Procedure/Guidance			Project
	Other – Please state			Code of practice
Geographical area covered	Trust-wide			
Aims and objectives	<p>This policy describes how personal confidential information should be protected or shared to:</p> <ul style="list-style-type: none"> <li>• ensure service users trust the organisation to respect their information;</li> <li>• ensure all staff understand when they must share information and when they should not;</li> <li>• provide the best quality healthcare by ensuring service users trust us enough to disclose personal confidential information;</li> <li>• ensure lives are not lost if information is not shared when it should be;</li> <li>• ensure we do not surprise service users with how we use their information.</li> </ul>			

Start date of Equality Analysis Screening	13 December 2019
End date of Equality Analysis Screening	13 December 2019

**You must contact the EDHR team if you identify a negative impact. Please ring Sarah Jay or Julie Barfoot on 0191 3336267/3046**

1. Who does the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan benefit?					
The policy benefits all individuals and organisations whose sensitive and personal information the Trust holds, transfers or processes					
2. Will the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan impact negatively on any of the protected characteristic groups below?					
<b>Race</b> (including Gypsy and Traveller)	No	<b>Disability</b> (includes physical, learning, mental health, sensory and medical disabilities)	No	<b>Sex</b> (Men, women and gender neutral etc.)	No
<b>Gender reassignment</b> (Transgender and gender identity)	No	<b>Sexual Orientation</b> (Lesbian, Gay, Bisexual and Heterosexual etc.)	No	<b>Age</b> (includes, young people, older people – people of all ages)	No
<b>Religion or Belief</b> (includes faith groups, atheism and philosophical belief's)	No	<b>Pregnancy and Maternity</b> (includes pregnancy, women who are breastfeeding and women on maternity leave)	No	<b>Marriage and Civil Partnership</b> (includes opposite and same sex couples who are married or civil partners)	No

**Yes** – Please describe anticipated negative impact/s

**No** – Please describe any positive impacts/s

Adhering to the policy will impact positively because we will only share personal information when there is a legal basis to do so. This will foster trust between data subjects and the organisation.

<p><b>3.</b> Have you considered other sources of information such as; legislation, codes of practice, best practice, nice guidelines, CQC reports or feedback etc.? <b>If 'No', why not?</b></p>	<b>Yes</b>	<b>X</b>	<b>No</b>	
---	------------	----------	-----------	--

- Sources of Information may include:**
- Feedback from equality bodies, Care Quality Commission, Equality and Human Rights Commission, etc.
  - Investigation findings
  - Trust Strategic Direction
  - Data collection/analysis
  - National Guidance/Reports

- Staff grievances
- Media
- Community Consultation/Consultation Groups
- Internal Consultation
- Research
- Other (Please state below)
- NHS confidentiality code of practice and data protection law.
- HSCIC code of practice on confidentiality.
- Caldicott Principles
- To share or Not to Share report

**4.** Have you engaged or consulted with service users, carers, staff and other stakeholders including people from the following protected groups?: Race, Disability, Gender, Gender reassignment (Trans), Sexual Orientation (LGB), Religion or Belief, Age, Pregnancy and Maternity or Marriage and Civil Partnership

**Yes** – Please describe the engagement and involvement that has taken place

Trust-wide consultation when developing the policy.

**No** – Please describe future plans that you may have to engage and involve people from different groups

5. As part of this equality analysis have any training needs/service needs been identified?

**No** Please describe the identified training needs/service needs below

A training need has been identified for;

Trust staff	No	Service users	No	Contractors or other outside agencies	No
-------------	----	---------------	----	---------------------------------------	----

**Make sure that you have checked the information and that you are comfortable that additional evidence can provided if you are required to do so**

The completed EA has been signed off by: You the Policy owner/manager: Type name: Theresa Parks	Date: 13/12/19
---	-------------------

Your reporting (line) manager: Type name: Louise Eastham	Date: 13/12/19
---	-------------------

If you need further advice or information on equality analysis, the EDHR team host surgeries to support you in this process, to book on and find out more please call: 0191 3336267/3046