Public – To be published on the Trust external website

Title: Sharing Information and Confidentiality policy

Ref:CORP-0010-v12

Status: Ratified
Document type: Policy

Contents

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. Sometimes information must be shared and confidentiality breached if it is in the best interests of a service user or in the public interest (Caldicott seventh principle). However a new 8th Caldicott Principle introduced in 2021 advises organisations to take steps to ensure there are no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this.

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*'.

Following this policy will ensure we only share information in a lawful way. Practitioners must balance patient confidentiality with the need to share information to provide the best care for our service users.

Our Journey To Change sets out why we do what we do, the kind of organisation we want to become and the way we will get there by living our values, all of the time. To achieve this, the Trust has committed to three goals. This policy supports all three goals of *Our Journey To Change*.

To co-create a great experience for patients, carers and families - implementing this policy provides assurance to patients, families and staff that when records are created the information

contained in them will be kept confidential but sharing information in a lawful way with service users will allow co-creation of the service user's record.

.

To co-create a great experience for our colleagues – this policy will ensure that all colleagues understand their role around the use and sharing of information that is created or used by them. When staff understand their roles and their duties they can be confident that the actions that they take are consistent and defendable. There is a delicate balance to be made between information sharing and confidentiality and this policy aims to support staff in making difficult decisions over whether to share or not to share.

To be a great partner - information and its governance is a key communication tool and is strategic in assisting the Trust when it works with key partners either to improve services or to jointly care for patients. When we tell our patients who we work with and have robust agreements about what is going to be shared we enable information to support outstanding care and service delivery with our partners.

Embedding our Journey to Change Goals will support our values of respect, responsibility and compassion.

2 Why we need this policy

We need this policy for staff to understand their responsibilities around information sharing and so that service users know what to expect from the Trust. 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 improve 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 law, UK Data Protection Act 2018 still recognises the importance of the common law duty of confidentiality.

Information is considered to be confidential when:

- The information has the necessary quality of confidence. All information does not have the same importance;
- The information must be imparted in circumstances giving rise to an obligation of confidence. For example, a service user disclosing health information about themselves to a doctor or nurse;
- There is unauthorised use of that information to the detriment of the original communicator of the information.

Please note the following regarding Gender Recognition Certificates:

- Under the Gender Recognition Act, information relating to a Gender Recognition Certificate is 'protected information' if it is acquired in a professional capacity like the NHS.
- It is an offence to disclose protected information to any other person unless an exemption applies.
- Some of the exemptions are the person has consented, the person cannot be identified from the information, information is needed for prevention and investigation of crime, information is needed to comply with a court order.
- Treat any information in relation to gender identity as protected information.
- Advice can be sought from Information Governance by emailing tewv.ig@nhs.net

The records of adopted individuals and individuals under witness protection also need to be protected. Do not share information that divulges adoption or witness protection status. For more information refer to the Trust's standards for clinical record keeping.

2.1 Purpose

The purpose of this policy is 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 information is shared when necessary to protect lives;
- ensure service users understand how we will use their information. There should be 'no surprises' for service users with regard to the use of their personal information.

2.2 Objectives

Following 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 principles.

3 Scope

This policy focuses on service user confidentiality, but all staff must understand that staff information may also be confidential. The Caldicott Principles relate specifically to patient identifiable information, however they can also be applied to staff identifiable information.

3.1 Who this policy applies to

This policy applies to all staff, students, volunteers and contractors. The policy has been reviewed with input from service users and students.

3.2 Roles and responsibilities

Role	Responsibility
Chief Executive	• Ultimate responsibility for all aspects of how information is collected, stored and used by the Trust to maintain confidentiality.
Caldicott Guardian	• 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 • 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. • The Trust's Caldicott Guardian is the Medical Director.
Data Protection Officer	• The Trust's Data Protection Officer is the Head of Information Governance. The Data Protection Officer upholds the Data Protection Act 2018.
Managers and supervisors	• Ensure 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.
Information Security Officer	• Facilitates 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 log of completed DPIAs.

Privacy Officer	• Monitors potential privacy breaches through the PARIS Break Glass function and monitors actual privacy breaches through the Close Monitoring procedure.
All staff, students, volunteers and contractors	• Maintains and protects the confidentiality of patient information which they use in their day to day roles. • Maintains confidentiality of staff and business information.

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)
- Human Rights Act 1998
- Mental Health Act 1983: Code of Practice
- Access to Health Records Act 1990 (protects the health information of deceased patients)

These laws 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 right to confidentiality.

Data Protection laws changed on the 25th May 2018 with the implementation of the Data Protection Act 2018. 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 Part 2, Chapter 2, paragraph 8 and Part 2, Chapter 2, paragraphs 10(1)(c) and 11(1a) and 11(2a and 2b) of the Data Protection Act 2018.

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.

The Trust relies on these as a lawful basis for processing 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 act (Data Protection Act 1998).

What this means is that when it is necessary to share personal information for the delivery of direct health care (refer to 'Definitions'), 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. The Privacy Notice will help to facilitate the conversation with the service user regarding the use of their confidential information. The conversation with the service user will ensure there are no surprises when using confidential service user information.

The conversation should include, for example:

- make clear to service users when information is recorded or health records are accessed;
- make clear to service users when they are or will be disclosing information with others;
- check that patients have no concerns or queries about how their information is disclosed and used.

Confidential information includes, but is not limited to the following:

- Address
- Health information such as a diagnosis
- Personal history – timeline of life events

The Data Protection Act 2018 is underpinned by 6 principles:

Accountability principle

We have put in place appropriate technical and organisational measures to meet the requirements of accountability. These include:

- The appointment of a data protection officer who reports directly to our highest management level.
- Implementing a 'data protection by design and default' approach to our activities
- Maintaining a record of our processing activities.
- Adopting and implementing data protection policies and ensuring we have written contracts and information sharing agreements in place with our partner organisations and joint data controllers.
- Implementing appropriate technical and organisational security measures for the personal data we process.
- Carrying out data protection impact assessments for our high risk processing and implementing risk mitigation actions.

We regularly review our accountability measures and update or amend them when required.

Principle (a): lawfulness, fairness and transparency

Processing personal data must be lawful, fair and transparent. It is only lawful if and to the extent it is based on law and either the data subject has given their consent for the processing, or the processing meets at least one of the conditions in Schedule 1. We provide clear and transparent information about why we process personal data including our lawful basis for processing in our privacy notice and this policy document. Our processing for purposes of substantial public interest is necessary for the exercise of a function conferred on the Trust by legislation. Our processing for the purposes of employment relates to our obligations as an employer. We also process special category personal data to comply with other obligations imposed on the Trust in its capacity as a public authority e.g. the Equality Act

Principle (b): purpose limitation

We will process data for the purpose it was provided to us as a health care provider or employer. If we are sharing data with another controller, we will document that they are authorised by law to process the data for their purpose. We keep a record of all data sharing. We will not process personal data for purposes incompatible with the original purpose it was collected for.

Principle (c): data minimisation

We ensure personal data collected is not excessive. The information we process is necessary for and proportionate to our purposes as described within the related Data Protection Impact Assessment(s). Where personal data is provided to us or obtained by us, but is not relevant to our stated purposes, we will erase it.

Principle (d): accuracy

Where we become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, we will take every reasonable step to ensure that data is erased or rectified without delay. If we decide not to either erase or rectify it, for example because the lawful basis we rely on to process the data means these rights don't apply, we will document our decision.

Principle (e): storage limitation

All special category data processed by us for the purpose of employment or substantial public interest is, unless retained longer for archiving purposes, retained for the periods set out in our retention schedule. We determine the retention period for this data based on our legal obligations and the necessity of its retention for our business needs. The Trust adheres to the retention schedule specified within the NHSX Records Management Code of Practice 2021.

Records that may or may not be of use for an inquiry must be retained until there is clear instruction from the inquiry. There are currently three independent inquiries which have requested that large parts of the health and social care sector do not destroy any records that are, or may fall into the remit of the inquiry

- The Infected Blood Inquiry - further information about the records required can be found on their website.
- UK COVID-19 Inquiry – this inquiry started in April 2021 and will examine, consider and report on preparations and the response to the pandemic in England, Wales, Scotland and Northern Ireland, up to and including the inquiry's formal setting-up date.

Principle (f): integrity and confidentiality

This policy applies regardless of the media on which data is held. All data is managed in line with the Trust's Information Security and Risk Policy. Electronic systems and physical storage have appropriate access controls applied as per the Access to Information Systems Policy and Physical Security Policy. The systems we use to process personal data are auditable and allow us to erase or rectify personal data at any point in time where appropriate.

The Trust's data security and protection arrangements are declared annually via the NHSD data security and protection toolkit which is subject to external audit and scrutiny. Our retention and disposal practices are set out in our retention and disposal policy available on the Trust's website.

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? The legal obligation for confidentiality is one of common law, which means it will change as case law evolves. In practice this will often mean that information cannot be disclosed without that person's explicit consent unless there is another valid legal basis.

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). This is published on the Trust's internet site. For example, service users may request a copy of their own clinical record. In the Trust it is the Data Protection Team who manage requests for personal information.

4.4 Confidentiality and Caldicott Principles

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?

4	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?
5	Everyone should be aware of their responsibilities	Do I understand this policy and other published literature on confidentiality including the HSCIC's 'A Guide to Confidentiality in Health & Social Care', 'Confidentiality: NHS Code of Practice' and the Information Governance Review: To Share or Not to Share.
6	Understand and comply with the law	Does what I'm sharing comply with the common law duty of confidentiality, data protection law (DPA 2018) and Human Rights Act 1998?
7	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?
8	Inform patients and service users about how their confidential information is used.	A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required.

4.5 Types of information that may be shared

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 should not 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. Members of the public may request an ISA through the Freedom of Information Act.

5 Consent

Consent can be defined as permission for something to happen or agreement to do something. Recital 32 of the UK General Data Protection Regulation states this about consent:

Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement.

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 'no surprises').

TEWV is legally obliged to be transparent about how personal information is used and shared. We must make information readily available to service users explaining how their information will be used, and their right to object. This is provided in our Privacy Notice. Refer to the section titled 'Privacy Notice' for further details.

In the NHS we talk about implied and explicit consent. We also talk about the lifecycle of consent.

Implied consent is consent which is not expressly granted by a person, but rather implicitly granted by a person's actions and the facts and circumstances of a particular situation.

Explicit consent must be expressly confirmed in words. Individuals do not have to write the consent statement in their own words; you can write it for them. However you need to make sure that individuals can clearly indicate that they agree to the statement – for example by signing their name or ticking a box next to it.

When confidential patient information is accessed and used for individual care then consent is implied, without the service user having to explicitly say so. This is because it is reasonable for service users to expect that relevant confidential patient information is shared with those caring for them on a need-to-know basis. The Trust does not rely on consent for delivering individual care and treatment. We rely on other legal bases for processing personal information enacted in the UK GDPR:

Article 6(1)(e) - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

Article 9(2)(h) - processing is necessary for the purposes of preventative or occupational medicine...medical diagnosis, the provision of health or social care or the management of health or social care systems and services…'

If confidential patient information is used for purposes beyond individual care, for example a research project, then it will normally be necessary to obtain explicit consent.

Consent to treatment is not covered in this policy. Please refer to Consent to Examination or Treatment policy for details of this topic. Consent for the use of person-identifiable images and information in Trust promotional and training materials is not covered in this policy. These documents are available from TEWV's internet site.

The lifecycle of consent – what does it mean and what do we have to do? Consent is not static. On one day a patient might agree to sharing specific information for an exact information sharing activity. The next day, week or month later, their consent to sharing for that specific purpose may change and they may dissent to the sharing. It is important that consent is recorded through its lifecycle. The lifecycle of consent can be divided into three distinct phases, collection, use and withdrawal. The important thing to do is to record dates of consent and dissent in the patient record in the Information Sharing module. It should be as easy to withdraw consent as it is to give consent.

Where processing personal information is based on consent, the consent is only valid if it is freely given, specific, informed and an unambiguous indication of the data subject's agreement to the processing of personal information. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them.

Consent is only appropriate where there is no other legal basis to rely on for the processing of personal information. Consent used a legal basis for processing should be used wisely because consent can be withdrawn at any time.

6 Privacy notice

For consent to be considered valid, data subjects should be informed of the data controller's identity, the purpose of the processing and how processing might affect them. Data subjects need to be told all purposes for processing their personal data before they give their consent.

You must give a Privacy Notice to service users on your caseload so there will be no surprises for them when we use their personal information. It is a legal obligation under data protection law to provide a Privacy Notice. There are a variety of Privacy Notices available from TEWV's internet site. We do not have an oral version of the Privacy Notice

but recommend that individuals use a screen reader to obtain an oral output of the document. There are a variety of screen readers available from the internet. When service users first have contact with TEWV services we do expect staff to discuss the use of their personal information so we comply with the eighth Caldicott Principle. It's important that staff understand if patients dissent to specific information sharing activities. Staff should periodically check information sharing preferences with service users to ensure consent is kept up-to-date.

The Information Sharing Module in the electronic patient record must be completed when a service user is referred to the Trust. You must check the Privacy Notice check box to show that you have provided a Privacy Notice.

7 Information sharing module in the electronic patient record

The information Sharing module in the electronic patient record captures the details of service user information sharing preferences. We must record when we provide a service user with a privacy notice by checking the Privacy Notice 'tick box'.

We must record the details of specific information sharing preferences. These have been divided into 'individual sharing preferences' and 'organisation sharing preferences'. These distinguish between sharing with individuals, e.g., a specific family member and sharing with organisations, e.g., a specific NHS Trust.

We must record when a service user dissents to sharing information, e.g., some service users may not want information shared with their family. Refer to Appendix 4 for instructions on recording information sharing preferences. It is important to know the date when someone withdraws their consent as this can change frequently for some patients. Some patients continuously change their mind regarding their sharing preferences.

8 Single Point of Contact for Information Sharing

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:

Kedar Kale
Executive Medical Director and Caldicott Guardian
Tarncroft
Lanchester Road Hospital
Lanchester Road
Durham
DH1 5RD
Telephone: 01325 552000
Email: TEAWVNT.AccessRequests@nhs.net

Single point of contact should not be confused with single points of contacts associated with service users or carers with regard to their communication with the Trust.

9 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.

10 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).

Service users should always know when their confidential information is being shared unless there is a good reason not to tell the service user.

11 Breaching confidentiality

All breaches of confidentiality will be investigated by the Trust.

Many breaches of confidentiality will be unintentional *e.g.*, sending group emails that share contact details without permission. In this situation, staff must contact information governance.

In the rare situation when 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 by the Information Commissioner and may be fined and other sanctions imposed.

12 Protecting information – environmental considerations

There are a number of practical measures we can take to ensure confidential information remains secure and is not inadvertently shared or disclosed so we can avoid personal data breaches. The measures we can take will depend upon the media we are using.

Paper information:

- Keep a clear desk.
- Use cross cut shredders to shred paper that holds person identifiable information. These shredders turn paper into coarse dust. Shredders which cut paper into ribbon-like strips must not be used because they do not meet the required standard.
- Use trust supplied confidential waste bins to dispose of paperwork that holds person identifiable information.
- Transport paper records in the locked boot of your car.
- Avoid taking paper records home. If you do have take home paperwork that contains person identifiable information then make sure it is always protected at home. Do not let others at home have access to your confidential paperwork.
- Do not keep confidential records or paperwork locked in your car during the day or overnight.

Electronic information:

- Lock your screen when you leave your computer. This advice applies at work and at home.
- Use encryption as advised by the Trust. Use encrypted, Trust supplied laptops. Use encrypted NHS mail when you have to send person identifiable information to a non-NHS mail address. In exceptional circumstances you may need to use a USB device. This must be encrypted to AES 256 bit encryption standard.
- Be mindful of where your computer screen is located both at work and at home. You do not want individuals to read your screen over your shoulder without you being unaware.
- Be mindful of where you situate white-boards in office spaces and what you record on them.

Conversations:

- Do not gossip about patients or staff.
- Hold sensitive conversations about confidential matters in private so you cannot be overheard.
- If you are working from home be mindful of who may be able to hear your private telephone conversations.
- When telephone callers contact you for personal information about patients or staff think carefully before you share any information over the telephone. You need to be assured that the caller has a justified need for the information. If there is a justified need, only share what is relevant and proportionate to the request.

13 Definitions

Term	Definition
Common law duty of confidentiality	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. 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.
Consent	The approval or agreement for something to happen after consideration. 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 '*no surprises*') 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. 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).
Data controller	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).
Data subject	The identified or identifiable living individual to whom the personal data relates.
Direct care	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.
Duty of confidence	Arises when one person discloses information to another (*e.g.* patient to clinician) in circumstances where it is reasonable to expect that the information will be held in confidence.
HSCIC	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.
Safe haven principles	The phrase "Safe Haven" originally referred to the siting of fax machines only; however the meaning has since been expanded to encompass all secure points at which confidential information is transferred between organisations, irrespective of purpose. The requirements for a safe haven include the following: • It should be to a room/area that is lockable or accessible via a coded key pad known only to authorised staff. • The room/area should be sited where only authorised staff can enter that location i.e. not an area accessible to all members of staff, or to visitors. • If the room/area is on the ground floor any windows should have locks on them. • The room/area should conform to health and safety requirements in terms of fire, flood, theft or environmental damage. • Computers should have adequate access controls such as password protection to qualify as a Safe Haven. • Personal passwords used to access computer systems containing confidential information should never be shared. • Computers should not be left on view or accessible to unauthorised staff, have a secure screen saver function and should be switched off when not in use.

14 Related documents

Communicating with service users best practice
Induction procedure
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

15 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 a line management briefing.
- The subject of confidentiality is 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'.

15.1 Training needs analysis

Staff/Professional Group	Type of Training	Duration	Frequency of Training
All staff, students and volunteers.	Information Governance	1 to 2 hours	Annual
Staff with specialist roles, e.g., Data Protection Officer, Caldicott Guardian.	Specialist training relating to role.	Varying but usually one day workshop.	Annual

16 How the implementation of this policy will be monitored

Number	Auditable Standard/Key Performance Indicators	Frequency/Method/Person Responsible	Where results and any Associate Action Plan will be reported to, implemented and monitored; (this will usually be via the relevant Governance Group).
1	Compliance with annual IG training.	Monitored through reports generated in the Integrated Information Centre. Monitored through the Trust's annual submission	Digital Performance and Assurance Group

		to the Data Security and Protection Toolkit.	

17 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: Public Interest Disclosures
Information Security Management: NHS Code of Practice
NHS Digital Information Sharing Resources
NHSx Information Governance Portal

18 Document control (external)

To be recorded on the policy register by Policy Coordinator

Date of approval	21 May 2024
Next review date	21 May 2027
This document replaces	CORP-0010-v12 Information Sharing and Confidentiality
This document was approved by	Digital Performance and Assurance Group (DPAG)
This document was approved	12 April 2024
This document was ratified by	Management Group
This document was ratified	21 May 2024
An equality analysis was completed on this policy on	12 January 2022
Document type	Public
FOI Clause (Private documents only)	N/A

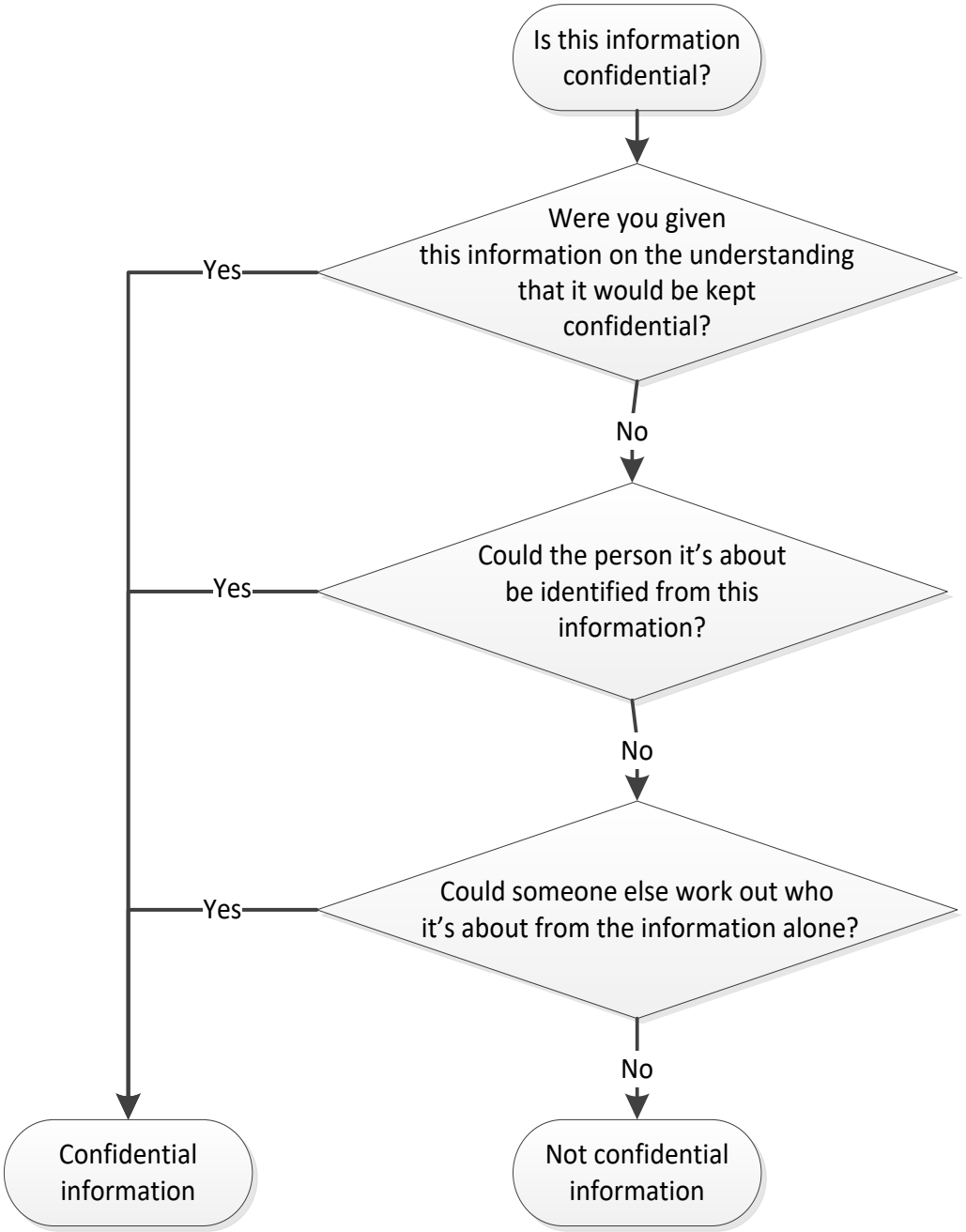
Change record

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.	Withdrawn
11	21 September 2022	8th Caldicott Principle added to the document. Safe haven requirements included. Text added to clarify specific points. Reference to GDPR removed. Hyperlinks checked and updated. Name of the document changed at this version. Added text on Gender Recognition Certificates.* Added text on adopted individuals and individuals under witness protection.*	Withdrawn

		Note * these two amendments arose from EIA review conducted by EDIHR Team after approval before ratification	
12	21 May 2024	• Updated and expanded the sections on Consent, Privacy Notice and Information Sharing Module Electronic Patient Record. • Added new section on Protecting Information – Environmental Considerations. • Added Cito screen shots of the Information Sharing Module to Appendix 4 • Added the 6 data protection principles at the request of Audit One auditor for Data Security and Protection Toolkit audit (07/03/2024) • Appendix 4 amended to remove reference to “Paris Change Release Note” as this has been superseded by Cito.* *change was made after 12 April 2024 DPAG meeting prior to ratification.	ratified

Appendices

Appendix 1: Determining confidentiality – decision support tree



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

Appendix 2: NHS Digital (HSCIC) Confidentiality Rules

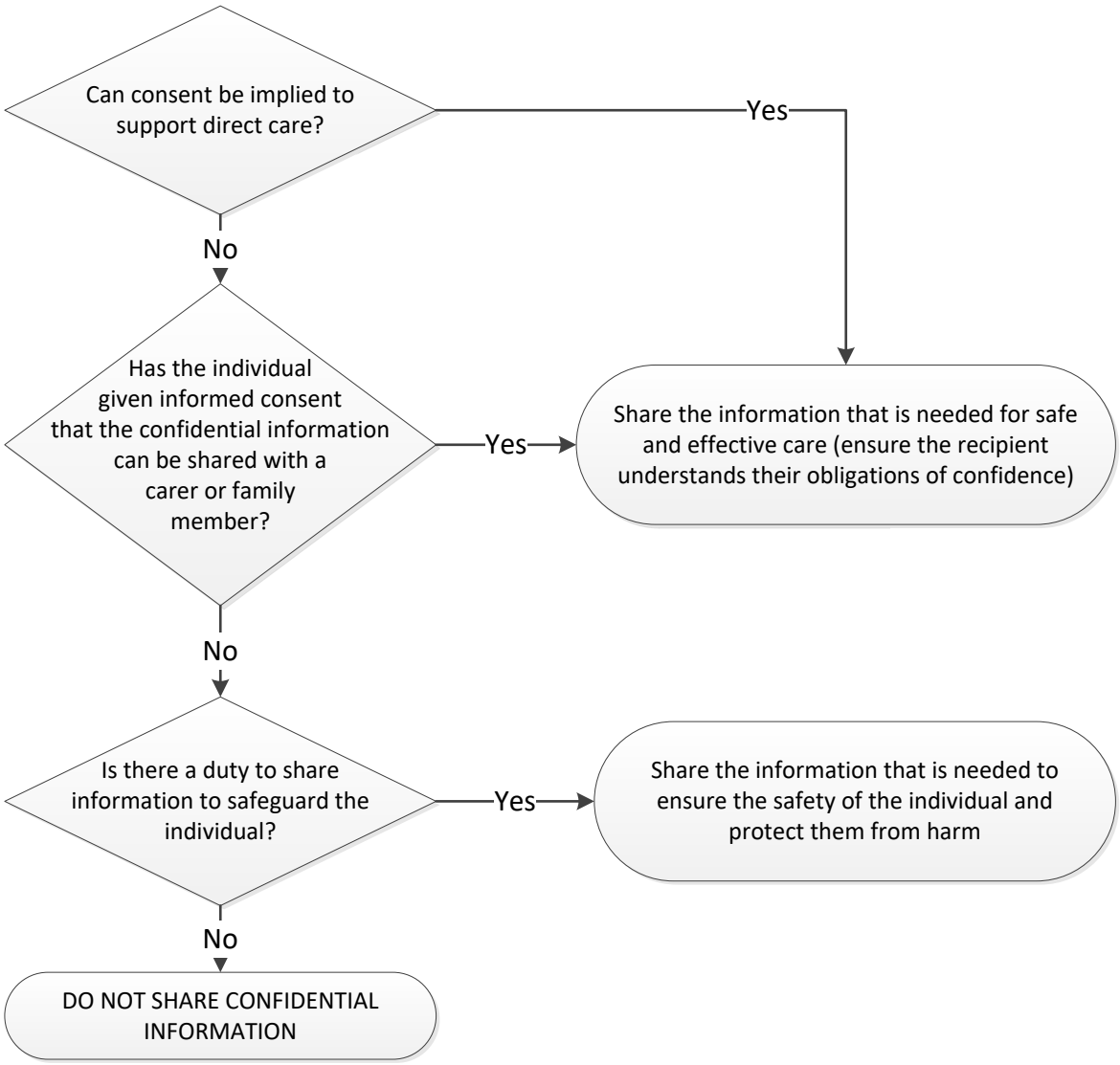
The Health and Social Care Information Centre (HSCIC) has established five confidentiality rules that people are entitled to expect to be followed in care settings run by the NHS or publicly funded adult social care services.

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. Safe haven principles are
- 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

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

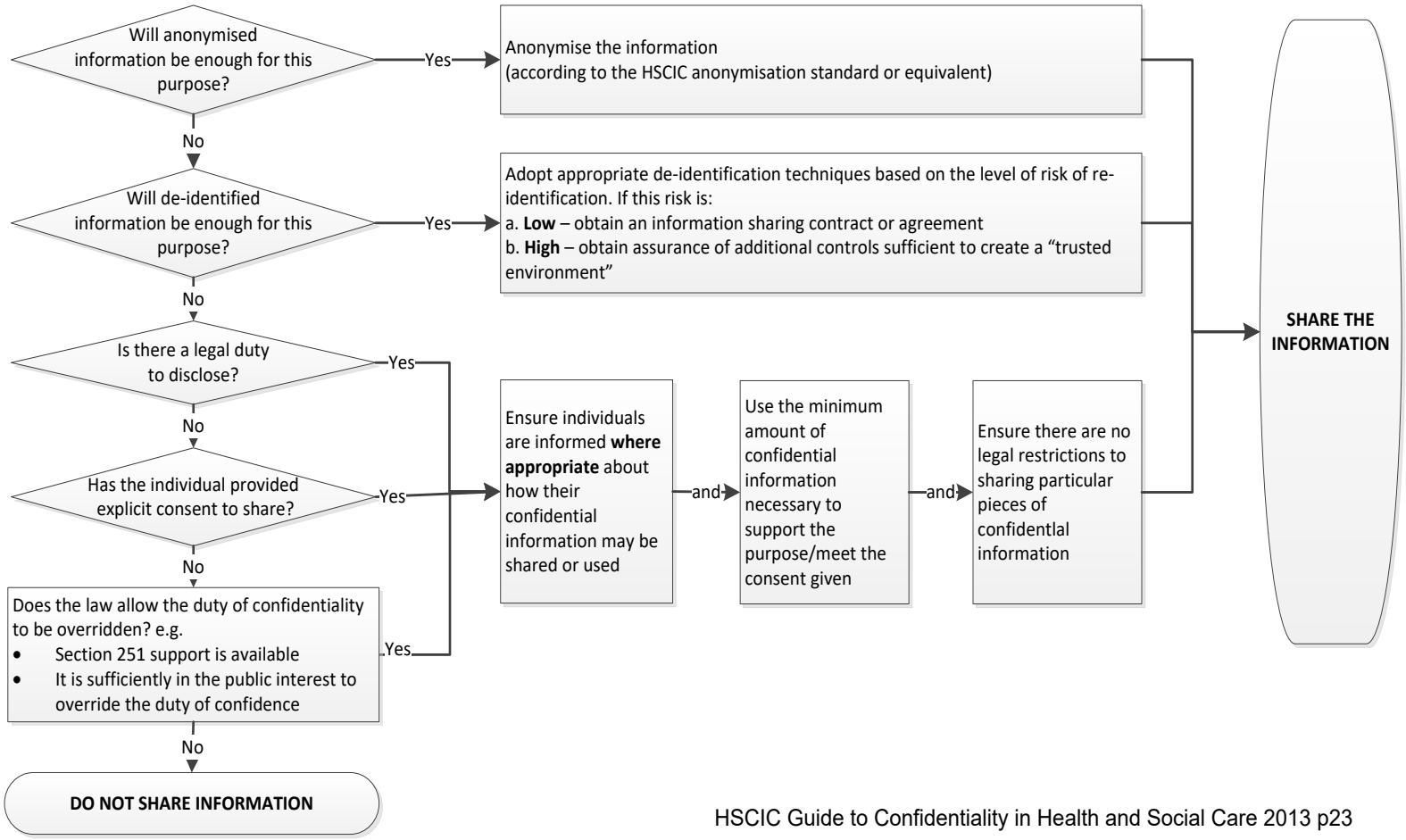


HSCIC Guide to Confidentiality in Health and Social Care 2013 p15

Note: consent is not needed for information sharing for the purpose of **direct care**.

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. In exceptional circumstances it may be necessary to use confidential information, but this requires informed consent of the individual or another legal basis which allows the sharing. For all lawful methods of sharing confidential information all of the following conditions should be met: • Individuals should be informed about how their confidential information may be used or shared. • Steps should be taken to use the minimum level of confidential information necessary to support the purpose. • The law should be checked to ensure there are no legal restrictions to sharing specific pieces of confidential information.

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

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.

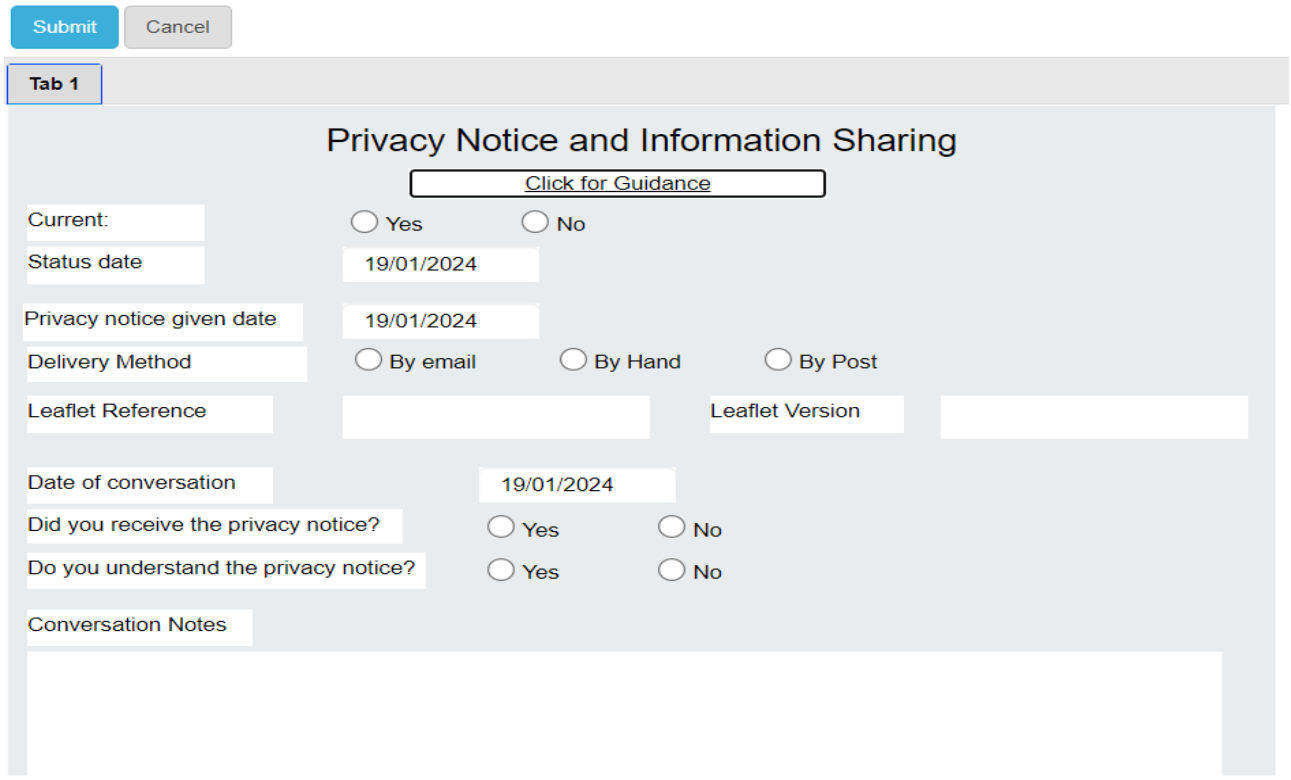
This guidance will be especially useful to support early intervention and preventative work where decisions about information sharing may be less clear than in safeguarding or child protection situations. The seven golden rules for information sharing are:

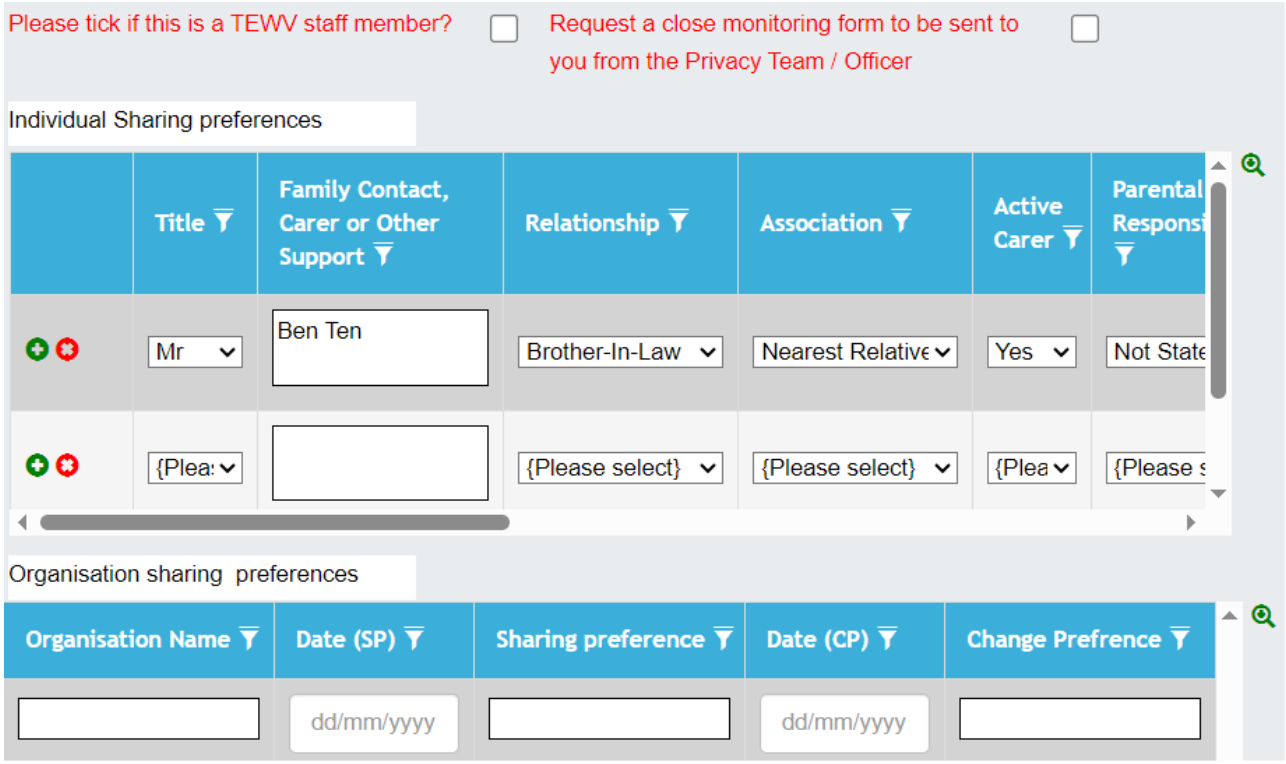
Rule 1 Remember that the Data Protection Act is not a barrier to sharing information but provides a framework to ensure that personal information about living persons is shared appropriately.
Rule 2 Be open and honest with the person (and/or their family where appropriate) from the outset about why, 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.

Appendix 4: Electronic patient record, information sharing module

CITO information sharing module screen shots

Launch new will start the form





Appendix 5: Equality Analysis Screening Form

Please note: The Equality Analysis Policy and Equality Analysis Guidance can be found on the policy pages of the intranet

Section 1	Scope
Name of service area/directorate/department	Information Governance
Title	Sharing information and confidentiality Policy
Type	Policy
Geographical area covered	Trustwide
Aims and objectives	To ensure that all patient information is processed fairly, lawfully and as transparently as possible so that the public • understand the reasons for processing personal information; • give their consent for the disclosure and use of their personal information; • gain trust in the way the NHS handles information and; • understand their rights to access information held about them.
Start date of Equality Analysis Screening	20 October 2021
End date of Equality Analysis Screening	12 January 2022

Section 2	Impacts
Who does the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan benefit?	It benefits service users and staff.
Will the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan impact negatively on any of the protected characteristic groups?	• **Race** (including Gypsy and Traveller) **NO** • **Disability** (includes physical, learning, mental health, sensory and medical disabilities) **NO** • **Sex** (Men, women and gender neutral etc.) **NO**

	• **Gender reassignment** (Transgender and gender identity) **NO** • **Sexual Orientation** (Lesbian, Gay, Bisexual and Heterosexual etc.) **NO** • **Age** (includes, young people, older people – people of all ages) **NO** • **Religion or Belief** (includes faith groups, atheism and philosophical beliefs) **NO** • **Pregnancy and Maternity** (includes pregnancy, women who are breastfeeding and women on maternity leave) **NO** • **Marriage and Civil Partnership** (includes opposite and same sex couples who are married or civil partners) **NO** • **Veterans** (includes serving armed forces personnel, reservists, veterans and their families **NO**
Describe any negative impacts	
Describe any positive impacts	The policy should enhance the trust between service users and staff. Staff will be able to make confident decisions regarding information sharing.

Section 3	**Research and involvement**
What sources of information have you considered? (e.g. legislation, codes of practice, best practice, nice guidelines, CQC reports or feedback etc.)	See references section
Have you engaged or consulted with service users, carers, staff and other stakeholders including people from the protected groups?	Yes
If you answered Yes above, describe the engagement and involvement that has taken place	This policy has been reviewed by a service user and a student nurse.
If you answered No above, describe future plans that you may have to engage and involve people from different groups	Note - The policy will be reviewed again by service users next time it is due for review.

Section 4	Training needs
As part of this equality analysis have any training needs/service needs been identified?	No - Confidentiality and information sharing are topics covered in annual information governance training.
Describe any training needs for Trust staff	No
Describe any training needs for patients	No
Describe any training needs for contractors or other outside agencies	No

Check the information you have provided and ensure additional evidence can be provided if asked

Appendix 6: Approval checklist

To be completed by lead and attached to any document which guides practice when submitted to the appropriate committee/group for consideration and approval.

	Title of document being reviewed:	Yes/No/ Not applicable	Comments
1.	**Title**		
	Is the title clear and unambiguous?	yes	
	Is it clear whether the document is a guideline, policy, protocol or standard?	yes	
2.	**Rationale**		
	Are reasons for development of the document stated?	yes	
3.	**Development Process**		
	Are people involved in the development identified?	yes	
	Has relevant expertise has been sought/used?	yes	
	Is there evidence of consultation with stakeholders and users?	yes	
	Have any related documents or documents that are impacted by this change been identified and updated?	yes	The IG Dept is reviewing all of its policies and procedures
4.	**Content**		
	Is the objective of the document clear?	yes	
	Is the target population clear and unambiguous?	yes	
	Are the intended outcomes described?	yes	
	Are the statements clear and unambiguous?	yes	
5.	**Evidence Base**		
	Is the type of evidence to support the document identified explicitly?	yes	
	Are key references cited?	yes	
	Are supporting documents referenced?	yes	
6.	**Training**		
	Have training needs been considered?	yes	
	Are training needs included in the document?	yes	
7.	**Implementation and monitoring**		

	Title of document being reviewed:	Yes/No/ Not applicable	Comments
	Does the document identify how it will be implemented and monitored?	yes	
8.	**Equality analysis**		
	Has an equality analysis been completed for the document?	yes	
	Have Equality and Diversity reviewed and approved the equality analysis?	yes	
9.	**Approval**		
	Does the document identify which committee/group will approve it?	yes	
10.	**Publication**		
	Has the policy been reviewed for harm?	yes	No harm identified
	Does the document identify whether it is private or public?	yes	Public
	If private, does the document identify which clause of the Freedom of Information Act 2000 applies?	n/a	Not applicable