Data Sharing Policy

Policy Domain	IMG
Policy ID	IMG 028
Version Number	7
Authors	Les De-Lara
Job Title	Information Governance Lead
First Release Date	10/10/2012
Ratification Date	20/08/2021
Ratified By	IT Steering Group
Implemented By	IT Steering Group
Audit and Review By	IT Steering Group
Review Frequency	Triennially
Last Review Date	05/08/2021
Next Review Date	By 01/08/2024

Table of Contents

REVISION SUMMARY

Version	Comments	Author	Date
V 1	Implementation of new policy for Healthshare.	IT Manager	10/10/2012
V2	Policy Review and Update	IT Manager	01/10/2013
V3	Policy Review and Update	IT Manager	01/10/2014
V4	Policy Review and Update	IT Manager	04/02/2016
V5	Policy Review and Update	IT Manager	01/02/2017
V6	Policy Review and Update	IM&G Manager	14/08/2018
V7	Policy Review and Update	IG Lead	05/08/2021

1 STATEMENT OF PURPOSE

This Data Sharing Policy outlines the guiding principles for information sharing, based on legal and ethical requirements. It aims to provide a framework for the secure sharing of patient-identifiable information between partner organisations and also covers wider issues of disclosing information to third parties.

As the nature of treatment and service delivery changes and there is an increasing emphasis on community care, health and social care organisations are becoming more inter-dependent and more reliant upon the sharing of information to provide services.

Information sharing can help to improve the quality of care and treatment, but it must be governed by the legal and ethical framework that protects the interests of patients. Without assurances of confidentiality, patients may be reluctant to provide the information needed for their treatment and care. Patients have a right to expect that information about them will be held in confidence and protected at all times against improper use and disclosure.

Patients have the right to know with whom information is going to be shared, and why. They also have the right to request that information is not shared – and staff must record these decisions in the clinical record.

2 RATIONALE

A review of the original Caldicott Report (1997) was completed and published in March 2013. The over-arching aim of the review was to ensure that there is an appropriate balance between the protection of personal confidential data/information, and use and sharing of such information to improve care.

The Caldicott Committee's *Report on the Review of Patient-Identifiable Information*, usually referred to as the **Caldicott Report** was a review commissioned in 1997 by the Chief Medical Officer of England due to increasing worries concerning the use of patient information in the National Health Service (NHS) in England and Wales and the need to avoid the undermining of confidentiality because of the development of information technology in the NHS, and its ability to propagate information concerning patients in a rapid and extensive way. There are 7 Caldicott Principles being:

- **Justify the purpose(s)**
  Every single proposed use or transfer of patient identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate guardian.

- **Don't use patient identifiable information unless it is necessary**
  Patient identifiable information items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

- **Use the minimum necessary patient-identifiable information**
  Where use of patient identifiable information is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out.

- **Access to patient identifiable information should be on a strict need-to-know basis**
  Only those individuals who need access to patient identifiable information should have access to

it, and they should only have access to the information items that they need to see. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes.

- **Everyone with access to patient identifiable information should be aware of their responsibilities**
  Action should be taken to ensure that those handling patient identifiable information - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

- **Understand and comply with the law**
  Every use of patient identifiable information must be lawful. Someone in each organisation handling patient information should be responsible for ensuring that the organisation complies with legal requirements.

- **The duty to share information can be as important as the duty to protect patient confidentiality**
  Professionals should in the patient's interest share information within this framework. Official policies should support them doing so.

The over-arching message within the document is that the public expect that relevant information related to their direct care should be shared within the care team (even if this includes professionals from other organisations): “Most people who use health and social care services accept and expect that doctors, nurses and other professionals will need to share personal confidential data if they are going to provide optimum care.” To care appropriately, you must share appropriately.

The Health and Social Care (Safety & 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. It makes it clear that “to share information can be as important as the duty to protect the patient”, and that unless an individual objects, information should be shared between professionals.

3 QUICK REFERENCE GUIDE

The Seven Golden Rules for Information Sharing (HM Government Information Sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers; July 2018) are:

3.1 **Remember that the General Data Protection Regulation (GDPR), Data Protection Act (DPA) 2018 and human rights law are not barriers to sharing information** but provides a framework to ensure that personal information about living persons is shared appropriately. The Health and Social Care (Safety & Quality) Act 2015 has introduced a “duty to share information” with regard to the provision of direct care.

3.2 **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.

3.3 **Seek advice** from other practitioners, or your Information Governance Lead, if you are in any doubt about sharing the information concerned, without disclosing the identity of the person where possible.

3.4 **Where possible, share with consent, and where possible, respect the wishes of those who do not consent to having their information shared.** Under the GDPR and DPA 2018 you may share information without consent if, in your judgement, there is a lawful basis to do so, such as where safety may be at risk. You will need to base your judgement on the facts of the case. When you are sharing or requesting personal information from someone, be clear of the basis upon which you are doing so. Where you do not have consent, be mindful that an individual might not expect information to be shared.

3.5 **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.

3.6 **Necessary, appropriate, 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.

3.7 **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.

4 SCOPE

This policy applies to all forms of records and information, regardless of medium that contain patient-identifiable data that may need to be shared between agencies and applies to all staff, services and processes performed by the Healthshare Group.

5 ROLES AND RESPONSIBILITIES

Healthshare's Caldicott Guardian is the officer responsible for overseeing all aspects of confidentiality and security in relation to patient-identifiable information.

All staff members that share information are obliged to adhere to this policy and guidelines. The unauthorised passing on of information pertaining to any individual is a serious matter. Unauthorised disclosure warrants consideration of disciplinary action and risks legal action by others. Health professionals may also be subject to action by their regulatory bodies.

Operationally, information sharing decisions will be made by the professional responsible for an individual's assessment, care or treatment, or on the advice of a senior professional or clinical supervisor within Healthshare, which may include the Caldicott Guardian.

Operation Directors at all levels are responsible for ensuring that the staff for whom they are responsible are aware of, and adhere to, this policy. They are also responsible for ensuring staff are updated in regard to any changes in this policy.

6 POLICY APPLICATION

Any service improvement, or transfer of service, that will/may involve the transfer/sharing/processing of personal information (staff or patient) should complete a Data Protection Impact Assessment. (Refer to IMG 027 Data Protection Impact Assessment)

6.1 Sharing information on a 'need to know' basis

- Sharing information should be on a 'need to know' basis in line with Caldicott Principle 4 [Refer to IMG 004 Data Protection and Confidentiality Policy].
- What is the purpose of the disclosure?
- What are the nature and the extent of the information to be disclosed?
- To whom is the disclosure to be made (and is the recipient under a duty to treat the material as confidential).
- Is the proposed disclosure a proportionate response to the need?
- Is the proposed disclosure legal – i.e. Is there a valid legal basis and/or exemption under the Data Protection Act 2018?

6.2 Sharing Information without consent

If a patient refuses to give consent to sharing information, or lacks capacity to consent, the individual's view should be respected except where disclosure is lawful without their consent. If the patient does not have capacity to consent to share – refer to the Mental Capacity Act training.

The following are examples of situations in which disclosure may be lawful without the consent of the patient:

- Where the information is required by statute or court order.
- Where disclosure is in the substantial public interest. This category of circumstances is not closed but the more common situations in which it will apply are:
  - When there is a serious risk to public health.
  - When there is a risk of serious physical/mental harm to the individual or those known to the individual.
  - For the prevention, detection or prosecution of serious crime (see definition below).
  - Where disclosure is necessary to protect vital interest i.e., where there is knowledge or belief of abuse or neglect of a child or vulnerable adult.
  - Circumstances detailed in any Dangerous Persons policy or guidance.
  - Where the disclosure is otherwise lawful e.g., covered by section 60 of the Health and Social Care Act.

6.3 Definition of Serious Arrestable Offences

Passing on information to help prevent, detect or prosecute serious crime may sometimes be justified to protect the public. There is no absolute definition of "serious" crime, but section 116 of the Policy and Criminal Evidence Act 1984 identified some "serious arrestable offences". These include:

- Treason.
- Murder.
- Manslaughter.
- Rape.
- Kidnapping.
- Certain sexual offences.

- Causing an explosion.
- Certain firearms offences.
- Taking of hostages.
- Hijacking.
- Causing death by reckless driving.
- Offences under the prevention of terrorism legislation.
- Making a threat, which if carried out, would be likely to lead to:
    - Serious threat to the security of the state or to public order.
    - Serious interference with the administration of justice or with the investigation of an offence.
    - Death or serious injury.
    - Substantial financial gain or serious financial loss to any person.

In other cases, legal advice should be sought through the DPO (Data Protection Officer) and SIRO (Senior Information Risk Officer) before taking a decision to release information.

For more information, refer to IMG 031 Disclosure of Information to the Police Procedure.

A decision to share or disclose information without consent must be recorded in detail, giving reasons for the decision made. The individual must be informed of the disclosure if he or she has the capacity to understand unless to do so would cause serious harm to the individual or someone known to them, or would prejudice the outcome of a criminal investigation or court proceedings.

6.4 Sharing Information for Purposes Other Than Treatment

Information that is disclosable by statute must be passed on by, or in consultation with, the professional responsible for the care of the individual. If in doubt, the advice of the DPO or SIRO must be sought.

Prior to releasing information for the protection of the public, the particular circumstances must be fully considered.

In deciding whether sharing information is in the public interest, staff will consider whether the release of the information to protect the public should prevail over the duty of confidence to the individual. In such circumstances, the advice of the DPO or SIRO must be sought.

Where there is any doubt about passing on information that may be disclosed by statute, or in any other circumstances that may justify passing on information without consent or statutory authority, the advice of the DPO or SIRO must be sought. The DPO or SIRO, in certain circumstances, may wish to seek legal advice, particularly if disclosure may result in a risk to the health of the individual or others known to them. The relevant professionals must be informed as soon as possible that information has been passed on, and the disclosure fully documented in the appropriate records including those of the patient. The individual must also be informed, unless to do so would cause serious harm to the individual or someone known to them, or would prejudice the outcome of a criminal investigation or court proceedings.

6.5 Sharing information requested by 3rd parties

There are occasions when 3rd parties request (e.g., police; solicitors, council etc.) information about data subjects – on occasion, this could simply be a request to confirm whether a data subject has been in contact

with any of Healthshare services. Disclosure of this information could be in breach of the Data Protection Act 2018, as it impacts on the rights and freedoms of the data subject.

Before ANY information is disclosed to the 3rd party, staff must:

- Confirm the identity of the 3rd party – i.e., by requesting a telephone number and confirming the identity of the requester.
- Establish whether the data subject has given their consent to the disclosure.
- Establish whether the 3rd party has provided a valid legal basis for the disclosure.
- Establish whether the 3rd party has provided a valid legal exemption to allow Healthshare to disclose the information.
- Staff must document the contact in detail and the decision-making process in the clinical record.

If in any doubt, staff must decline to provide the information, and seek advice from the DPO or SIRO.

6.6 Sharing Information with consent

Sharing of information should, where possible, be with the consent of the patient.

Patients should be informed of the purposes for which information about them may be recorded and shared. It is only with sufficient information that consent may be given.

Patients should be given an opportunity to express their wishes as to how information should be used and these wishes should be respected where possible.

6.7 Patient Consent

Consent to share information must be sought from patients in a sensitive manner. At all times the rights, interests and dignity of the patient must be respected. Patients must have the opportunity to discuss any aspects of information sharing that are specific to their treatment and personal circumstances.

Staff will inform patients of how information will be used before they are asked to provide it. This includes informing patients of the kinds of purposes for which information about them is collected, and the types of people and agencies to which information may need to be passed, such as clinicians.

Consent to share information must be recorded in the patient's clinical record.

Consent should be sought at the earliest opportunity. This should be at the first contact with the patient unless the patient is unable, at that time, to comprehend the procedures or make an informed judgement. Cases in which the patient is incapacitated are dealt with in 6.3.

Once consent to share personal information has been obtained, it will be assumed to continue unless the patient withdraws consent but will be limited to the purposes for which consent was given.

A patient's case file or other personal record should always be checked for evidence of consent before personal information is shared with another agency.

Healthshare recognises that is it not practicable to seek a patient's (or other informant's) specific consent each time information needs to be passed on for the routine provision of care or delivery of a care plan. However, patients should be made aware of the purposes to which information about them may be put and this should mean that a patient is not surprised to find out how information about them has been used. If these conditions are not met then the sharing of information may be in breach of confidence or the General Data Protection Regulations. Staff should take further advice if there is any doubt over the circumstances surrounding such disclosures.

6.8 Refusal of Consent

Individuals have the right to object to the information they provide in confidence being disclosed to a third party in a form that identifies them, even if the third party is someone who might provide essential healthcare. Where individuals are competent to make such a choice and where the consequences of the choice have been fully explained, the decision should be respected. This is no different from a patient exercising his or her right to refuse treatment.

There are a number of issues to consider if a patient refuses to consent to information sharing:

- The concerns of the individual must be clearly established and attempts made to find out whether there is a technical or procedural way of satisfying these concerns without unduly compromising care.
- The options for providing an alternative form of care or to provide care through alternative arrangements may need to be explored.
- Decisions about the options for alternative arrangements that might be offered to the patient have to balance the risks, staff time and other costs that may result against the risk to the individual of not providing assessment, care or treatment.

Careful documentation of the decision-making process and the choices made by the individual must be documented in the individual's records.

6.9 Consent cannot be obtained (for reasons other than refusal)

In some circumstances it may not be possible to obtain consent because, in the opinion of the person responsible for the patient's care or well-being, the patient:

- Is too ill.
- Does not have the capacity to consent as per the Mental Capacity Act.
- The situation is urgent and the individual cannot be located to obtain consent.

In such cases, Healthshare recognises that it may be necessary to share information with other agencies so that appropriate care and treatment can be provided to the individual, or in exceptional circumstances where disclosure would be in the public interest - for instance where disclosure of the information is necessary to prevent harm coming to another individual.

When seeking consent from individuals whose disabilities or circumstances prevent them from being informed about the likely uses of their personal information, it may be necessary to provide advice to the individual in a suitable format or language that is accessible. Checks must be made to ensure that the advice has been understood. Consent, or refusal of consent must then be documented in the individual's case records.

Some individuals may have difficulty communicating their decision to give consent or to withhold it. In this case, a clear and unambiguous signal must be provided of what is desired by the individual. Confirmation of the choice made may be obtained by repeating back the choice so that the individual can indicate assent. Failure to provide such support could be an offence under the Disability Discrimination Act 1995 and may prevent valid consent from being gained.

If an individual is unconscious or unable, due to a mental or physical condition, to give informed consent or to communicate a decision, staff must take decisions about the use of information. This will take into account the individual's 'best interests' (see 6.11 below) and any previously expressed wishes, informed by the views of relatives or legally responsible persons as to the likely wishes of the individual. Consent, or refusal of consent, must be documented in the individual's case records.

Individuals may be asked to indicate the person they would like to be involved in decisions about their care should they become incapacitated. This will normally, but not always, be the 'next of kin' or their carer. Limited information, on the basis of 'need to know' or 'best interests' of the individual, may be shared with that person provided the individual does not object. This gives individuals the opportunity to agree to disclosures or to choose to limit disclosure, if they so wish.

Where consent cannot be gained because it is not practicable to locate or contact an individual, this must be well evidenced and documented in the patient's clinical record.

6.10 Sharing information when abuse of vulnerable adults is suspected

The duty to report abuse of vulnerable adults' over-rides the normal responsibility to respect confidence. The following principles from the Caldicott Committee "Report on the review of patient-identifiable information" apply. The interests and welfare of the adult at risk are paramount. Information will only be shared on a "need to know" basis when it is in the best interests of the patient.

Confidentiality must not be confused with secrecy. Consent to share information should be sought, but if this is not possible and other vulnerable adults are at risk, it may be necessary to over-ride the requirement. It is inappropriate for agencies to give assurances of absolute confidentiality in cases where there are concerns about abuse, particularly those situations where other vulnerable people may be at risk. Disclosure of personal information will need to be in accordance with the General Protection Regulations where this applies.

6.11 Acting in a person's best interests

The following factors must be considered in determining a persons' best interests:

- The ascertainable past and present wishes and feelings of the person concerned and the factors the person would consider if able to do so.
- The need to permit and encourage the person to participate or improve his/her ability to participate as fully as possible in anything done for and any decision affecting him or her.
- The views of other people whom it is appropriate and practical to consult about the person's wishes and feelings and what would be in his/her best interest.
- Whether the purpose for which any action or decision is required can be as effectively achieved in a manner less restrictive of the persons freedom of action.

- Whether there is a reasonable expectation of the person recovering capacity to make the decision in the reasonably foreseeable future – and there is no immediate need for action to be taken.
- The need to be satisfied that the wishes of the person without capacity were not the result of undue influence.

6.12 Sharing Information with Families

Healthshare supports working closely with families. Obtaining information from and listening to the concerns of families are key factors in determining risk. We recognise, however, that some people do not wish to share information about themselves or their care. Practitioners should therefore discuss with people how they wish information to be shared, and with whom. Wherever possible, this should include what should happen if there is serious concern over suicide risk.

Healthshare want to emphasise to practitioners that, in dealing with a suicidal person, if they are satisfied that the person lacks capacity to make a decision whether to share information about their suicide risk, they should use their professional judgement to determine what is in the person's best interest.

It is important that the practitioner records their decision about sharing information on each occasion they do so and also the justification for this decision.

Even where a person wishes particular information not to be shared, this does not prevent practitioners from listening to the views of family members, or prevent them from providing general information, such as how to access services in a crisis.

6.13 Young People

There will be instances when staff will be expected to share information with professionals working with young people for the purposes of Safeguarding and promoting the welfare of young people. In most instances this will be done with the consent of the patient but there may be situations when information will need to be shared without the child or parent's consent.

Young people aged 16 or 17 are regarded as adults for the purposes of consent and are therefore entitled to the same requirements for confidentiality as adults. Staff will ensure that consent for the sharing of information with other agencies is obtained from young people aged 16 or 17 on the same basis as adults.

6.14 Patients' Access to their own Records

Individuals, subject to certain safeguards, have a right to access their personal records under the Data Protection Act 2018. Healthshare will ensure that it complies with the requirements of the Data Protection Act 2018 in terms of requests to access personal identifiable information.

6.15 Breaches of confidentiality

If staff become aware that a breach of this policy and/or confidentiality occurs, they must:

- Log the incident on the Healthshare Intranet.
- If considered a serious breach – inform the Information Governance Lead.

- The ITSG will co-ordinate an investigation with the manager and assess the seriousness of the incident. If required, this will be reported to the Caldicott Guardian, at least one senior member of the Healthshare Directorate, and the Commissioners and the Information Commissioners Office.
- Any learning from these incidents will be shared with the SLT by the IT Applications and Data Lead.

6.16 Indemnity

Disclosure of personal information without consent must be justifiable on statutory grounds, or meet the criterion for claiming an exemption under the General Data Protection Regulations. Without such justification, both Healthshare and the member of staff expose themselves to the risk of prosecution and liability to a compensation order under the General Data Protection Regulations or damages for the breach of the Human Rights Act.

7 MONITORING AND AUDIT

Monitoring/audit arrangements	Methodology	Reporting		
		Source	Committee	Frequency
That due process is followed in line with this Policy	Internal Review	IG Lead	IT Steering Group	3 yearly

8 EQUALITY IMPACT STATEMENT

During the development of this policy the Company has considered the needs of each protected characteristic as outlined in the Equality Act (2010) with the aim of minimising and if possible, remove any disproportionate impact on employees for each of the protected characteristics, age, disability, gender, gender reassignment, pregnancy and maternity, race, religion or belief, sexual orientation.

If staff become aware of any clinical exclusions that impact on the delivery of care an incident form would need to be completed and an appropriate action plan put in place

Equality Impact Assessment

The Company aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others. The Equality Impact Assessment tool assesses the impact of this policy.

		Yes/No	Comments
1.	Does the document/project affect any group less or more favourably than another on the basis of:		
	• Disability	No	
	• Sex	No	

	• Race	No	
	• Age	No	
	• Gender Reassignment (including transgender)	No	
	• Sexual orientation	No	
	• Pregnancy & Maternity	No	
	• Other identified groups	No	
2.	Is there any evidence that some groups are affected differently?	No	
3.	If you have identified potential discrimination, are there exceptions valid, legal and/or justifiable?	No	
4.	Is the impact of the document/project likely to be negative?	No	
5.	If so can the impact be avoided?	NA	
6.	What alternative is there to achieving the document/project without impact?	NA	
4.	Can we reduce the impact by taking different action?	NA	

Completed by:

Name	**Position**	**Date Completed:**
Les De-Lara	**IG Lead**	**05/08/2021**

9 REFERENCES

REFERENCES	General Data Protection Regulation The Data Protection Act 2018 Mental Health Act 1983 (As amended The Human Rights Act 1998 The Regulation of Investigatory Powers Act 2000 The protection of Freedoms Act 2012 Caldicott Report
RELATED POLICIES	Business Continuity Policy Data Protection Policy Data Protection and Confidentiality policy Data Protection Impact Assessment Procedure