Family Nursing & Home Care

Information Sharing Policy

January 2023

Document Profile

Document Registration	Added following ratification
Type	Policy
Title	Information Sharing Policy
Author	Head of Information Governance & Systems
Category	Information Governance
Description	Information Sharing Policy
Approval Route	Organisational Governance Approval Group
Approved by	Rosemarie Finley
Date approved	4 January 2023
Review date	3 years from approval
Document Status	This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled. As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the intranet.

Version control / changes made

Date	Version	Summary of changes made	Author
January 2023	1	New policy	Claire Whelan

CONTENTS

1 INTRODUCTION

1.1 Rationale

In a healthcare setting sharing information in line with agreed protocols can add a number of benefits. It can contribute towards making services more efficient and accessible to those in need. It ensures that all patients, including the vulnerable, are provided with the protection they need. It also enables collaboration amongst different organisations so that they can deliver the care that all patients, including those with complex needs, may be reliant upon.

Sharing information can present risks which must be adequately managed at every stage. Information systems are consistently becoming more complex and widespread with the potential for more information about individual's private lives, which is often highly sensitive, to become known to more and more people.

This Information Sharing Policy details the obligations and commitments that staff must follow at all times to ensure that legislation is not breached and that patients/families/carers/staff/employee's confidentiality is maintained at all times.

It sets out the principles and commitments that will underpin the secure and confidential sharing of information in delivering health and social care, in accordance with local policy and legislative requirements.

The main objectives of this policy are to:

- provide a framework to clarify procedures relating to the safe sharing of information
- ensure that everyone working with personal information fully understands the importance of information sharing, where it improves care for service users and for the direct continuing care of service users
- ensure that only the minimum amount of information deemed necessary for the purpose of the delivery of a care episode is, and should be, shared
- ensure that when information sharing occurs, this complies with the law, stipulated guidance, best practice and agreed protocols to ensure that service users' rights are respected
- ensure that confidentiality is adhered to unless there is a robust public interest in disclosure or a legal justification to do so

1.2 Scope

This policy applies to all staff employed by Family Nursing & Home Care (FNHC), including Committee members, seconded staff, bank staff, students on temporary placement and contractors.

1.3 Roles and Responsibilities

The Committee

The Family Nursing & Home Care Committee is collectively known as the 'Data Controller'. They permit the organisation's staff to use computers and relevant filing systems (manual records) in connection with their duties.

Chief Executive Officer (CEO)

The CEO has overall accountability for the management of information governance and the sharing of information within FNHC.

Director of Governance and Care

The Director of Governance and Care has a particular responsibility for ensuring that FNHC corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements. They also act as the Caldicott Guardian for the organisation (see below).

Senior Information Risk Officer (SIRO)

The CEO acts as FNHC's SIRO and has overall responsibility for the organisation's Information Risk Management (IRM). The SIRO also leads and implements the Information Governance (IG) risk assessment and advises the Committee on the effectiveness of IRM across the organisation.

Head of Information Governance and Systems

They are responsible for ensuring a fit for purpose and ratified policy is in place and for ensuring that the procedures and controls required in support of this policy are developed and maintained. They are responsible for managing associated risks and escalating to the appropriate person where necessary. They also act as the organisation's Data Protection Officer (DPO).

Caldicott Guardian

The Director of Governance and Care is FNHC's Caldicott Guardian. They have a particular responsibility for protecting the confidentiality of people's healthcare data. They are responsible for ensuring it is shared in an appropriate and secure manner.

Line Managers

All the managers across the organisation's business units are directly responsible for:

- Ensuring their staff are made aware of this policy and any notices
- Ensuring their staff are aware of their data protection responsibilities
- Ensuring their staff are aware of their Caldicott responsibilities

- Enable their staff to receive suitable information governance training
- Monitoring compliance with the requirements of this policy within their team

All Staff

All staff must comply with this policy and report data breaches to their line manager and on ASSURE in line with the Information Governance Policy.

2 POLICY

2.1 Key Principles

In the UK Government response to the Caldicott Review, it is stated that "The duty to share information can be as important as the duty to protect patient confidentiality" (DofH 2013 p5). Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by the Caldicott Principles. They should be supported by the policies of their employers, regulators and professional bodies.

All employees working within FNHC are bound by the common law duty of confidence and must comply with data protection legislation. Staff must handle personal information they may come into contact with during the course of their work in a lawful and compliant manner. This is not just a requirement of their contractual responsibilities but also a requirement within the common law duty of confidence and data protection legislation.

Information can relate to patients, staff (including temporary staff), members of the public, or any other identifiable individual, however stored. Information may be held on paper, CD/DVD, USB sticks, computer file or printouts, laptops, palmtops, mobile phones, digital cameras or even heard by word of mouth.

In all circumstances of information sharing staff will ensure the following:

- ✓ Individuals' rights will be respected, particularly confidentiality, security and the rights established by the Data Protection (Jersey) Law 2018
- ✓ When information needs to be shared, sharing complies with the law, guidance, best practice is followed and an information sharing agreement is in place
- ✓ Reviews of information sharing should be undertaken to ensure the information sharing is meeting the required objectives/purpose and is still fulfilling its obligations
- ✓ Confidentiality must be adhered to unless there is a robust public interest or a legal justification in disclosure
- ✓ Only the minimum information necessary for the purpose will be shared

2.2 Types of Data that can be shared

For the purpose of this policy, there are essentially three types of data. These are:

- Personal Data
- Special Category Data
- Anonymised and Aggregated Data

Wherever possible anonymised or aggregated data should be used, unless there is legitimate reason for sharing personal and special category data.

2.2.1 Personal Data

Data Protection legislation only applies to personal data about a living, identifiable individual. However, the definition of personal data is highly complex and for day-to-day purposes it is best to assume that all information about a living, identifiable individual is personal data.

Such personal data might include, but not be limited to:

- ✓ Name
- ✓ Address
- ✓ Telephone Number
- ✓ Age
- ✓ A unique reference number such as EMIS number or payroll number

The Data Protection (Jersey) Law 2018 imposes obligations and restrictions on the way that the organisation processes personal data. Data Protection legislation regards 'processing' of data to include collecting, storing, transmitting, amending and disclosing data.

The individual who is the subject of the data (the 'Data Subject') has the right to know who holds their data and how such data will be processed, including how such data is to be, or has been, shared. It is the responsibility of the data processer to communicate this appropriately, for example at the point the data is collected, and through FNHC's Privacy Policy.

2.2.2 Special Category Data

The Data Protection (Jersey) Law refers to certain types of data as 'Special Category Data' for example:

- Ethnic origin
- Political opinions
- Religious beliefs
- Trade union membership
- Genetics
- Biometrics
- Health
- Sexual orientation

Conditions for processing are set out in Schedule 2 (Article 9) of the Data Protection (Jersey) Law 2018.

2.2.3 Anonymised and Aggregated Data

Anonymised and aggregated data can be used in very similar ways.

Anonymised data are individual records from which the personal identifiable fields have been removed.

Aggregated data which has been processed to produce a generalised result, from which individuals cannot be identified. However, care must be taken when such aggregations could lead to an individual being identified e.g. groupings with small distribution leading to isolation of individual's characteristics.

Anonymous or aggregate information may be shared internally or with other organisations. For example this could be to improve patient experience; facilitate contracts of services; manage and plan future services; facilitate quality improvement and clinical leadership; assure and improve the quality of care and treatment; statutory returns and requests; train staff; audit performance.

Effective anonymization techniques should be used to provide a privacy-friendly alternative to sharing personal data (ICO 2021).

2.3 Information Sharing Agreements

Information sharing agreements, sometimes known as 'Information sharing protocols' or 'data sharing protocols', set out a common set of rules to be adopted by the various organisations involved in an information sharing operation.

These could well form part of a contract between organisations. It is good practice to have an information sharing agreement in place, and to review it regularly, particularly where information is to be shared on a large scale, or on a regular basis.

An information sharing agreement must, at least, document the following:

- the purpose or purposes of the sharing
- the legal basis for sharing under the DPJL 2018
- the legal basis to comply with the common law duty of confidence
- the potential recipients or types of recipient and the circumstances in which they will have access
- who the data controller(s) is and any data processor(s)
- the data to be shared
- data quality – accuracy, relevance, usability
- data security
- retention of shared data
- individuals' rights – procedures for dealing with access requests, other applicable
- DPJL 2018 rights, queries and complaints
- review of effectiveness/termination of the sharing agreement

- any particular obligations on all parties to the agreement, giving an assurance around the standards expected
- sanctions for failure to comply with the agreement and/or breaches by individual staff

An information sharing agreement should be used when FNHC act as data controller, is sharing information directly with other organisations that will act either as a joint data controller with FNHC, or as data controllers in their own right for that information.

Any processing by an organisation on behalf of FNHC shall be governed by a data processing agreement. The Data Protection (Jersey) Law 2018 requires a contract that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.

The Caldicott Report (1997) and subsequent Review (DofH 2013) recommended that information sharing agreements should be developed between organisations sharing personal identifiable information.

2.4 Data Protection Impact Assessment

Before establishing a new process that involves processing of personal data including information sharing, a Data Protection Impact Assessment (DPIA) must be conducted.

A DPIA helps to assess the benefits that the information sharing might bring to particular individuals or society more widely, balanced against any risks to individuals arising from processing their data. It also ensures that the appropriate legal bases are identified and documented.

It identifies risks or potential negative effects, such as non-compliance with data protection legislation, an erosion of personal privacy, or the likelihood of damage, distress or embarrassment being caused to individuals.

As well as harm to individuals, staff should consider potential harm to the organisation's reputation which may arise if information is shared inappropriately, or not shared when it should be.

Any new information assets and data flows that arise out of a new project or procurement where FNHC is the data controller or receives personal, confidential, sensitive or business-sensitive information will need to be recorded as part of FNHC's Information Asset Register.

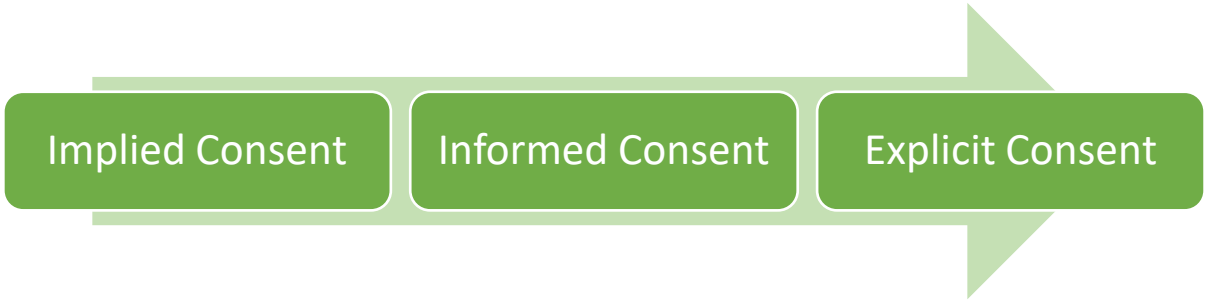
3. PROCEDURE

3.1 Consent to Information Sharing

When disclosing personal information, many of the data protection issues surrounding disclosure can be avoided if the consent of the individual has been sought and obtained.

The general principle is that information will only be shared with the consent of the subject of the information. Consent must be freely given after the alternatives and consequences are made clear to the person from whom permission is being sought.

There are three types of consent relevant to information sharing:



- Implied Consent – the individual has not been specifically asked if they wish to share or not share their information/record but the permission is set in the system to allow the sharing to happen. This will usually be done by a clinician who feels it in the individual's best interests, due to their care needs or mental incapacity

- Informed Consent – the individual is fully aware of why their information will be shared, how this will be done, who will the information be shared with and how the information will be used

- Explicit Consent – the individual is specifically asked if they wish to share or not share their information/record. The individual agrees that "yes" they are happy for their information/record to be shared.

If the data is classified as sensitive data (Special Category Data) the consent must be explicit. In any case the specific detail of the processing should be explained to the individual. This should include:

- Precisely who is processing the data
- The particular types of data to be processed
- The purpose of the processing
- Any special aspects of the processing which may affect the individual e.g. disclosures
- The person/agencies to whom the information will be made available

In the absence of consent, the practitioner must balance the duty of care, the public duty of confidentiality and Human Rights of the individual against the need to prevent and detect crime and disorder, and serve the public interest, in order to make a positive decision whether or not to release the information.

Where consent of the individual is not sought, or is sought but withheld, there can still be an exchange of information where there is an overriding public interest or justification for doing so.

If informed consent has not been sought, or has been sought and withheld, the practitioner must consider if there is any other overriding factor for the justification for the disclosure.

In making this decision the following should be considered:

- Is the disclosure necessary for the prevention or detection of crime, prevention of disorder, to protect public safety, or to protect the freedoms of others?
- Is the disclosure necessary for the protection of a child or a vulnerable adult?
- What risk is posed to others by this individual?
- What is the vulnerability of those who may be at risk?
- What will be the impact of the disclosure on the subject and on others?
- Is the disclosure proportionate to the intended aim?
- Is there an equally effective but less intrusive alternative means of achieving that aim?

Best Interests

To achieve this shared vision and fulfil the overriding objective of the Children and Young People (Jersey) Law 2022, proactive information is essential to effectively safeguard the welfare and promote the wellbeing of children and young people. Where information is not shared, or the protocol for sharing is not followed, responsible partners and relevant providers may miss opportunities to act to keep children and young people safe.

Practitioners should have the confidence to share information for the purpose of safeguarding. Guidance has been designed to assist practitioners to determine when and how information should be shared and on what basis. When sharing information, practitioners should follow the Best Practice Principles for information sharing, outline in the Children and Young People (Jersey) Law 2022 (jerseylaw.je)

In making a decision the following should be considered:

- To establish whether there is a clear and legitimate purpose to share information, practitioners should consider the following:

- In order to act in the best interests of this child, do I need to share this information with another party?

- Could sharing this information promote and support the wellbeing, and safeguard the welfare, of this child or young person?

- Am I responsible for making this decision around information sharing?

- In each case, practitioners should consider the impact of sharing information on the child or young person, in both the immediate and long term.

- When making decisions around information sharing, practitioners must always have the best interests of the child as a primary consideration in line with a children's rights approach

3.2 Process of Information Sharing

3.2.1 Systematic Information Sharing

This will generally involve routine sharing of data sets between organisations for an agreed purpose. It could also involve a group of organisations making an arrangement to 'pool' their data for specific purposes.

3.2.2 Exceptional or 'one-off' information sharing

Much information sharing takes place in a pre-planned and routine way. As such, this should be governed by established rules and procedures. However, departments/staff may also decide, or be asked, to share information in situations which are not covered by any routine agreement.

In some cases this may involve a decision about sharing being made in conditions of real urgency, for example in an emergency situation. All ad-hoc or one-off sharing decisions must be carefully considered and documented.

Requests for information from third parties i.e. GoJ Police Dept, Court and Legal firms must be sent to the Director of Governance & Care without delay for processing.

3.3 Factors to consider

When deciding whether to enter into an arrangement to share personal data either as a provider, a recipient or both, the following factors should be considered.

What is the sharing meant to achieve?	There should be a clear objective or set of objectives. Being clear about this will identify the following.
Could the objective be achieved without sharing the data or by anonymising it?	It is not appropriate to use personal data to plan service provision, for example, where this could be done with information that does not amount to personal data.
What information needs to be shared?	You should not share all the personal data you hold about someone if only certain data items are needed to achieve the objectives. The third Caldicott principle specifies "Use the minimum necessary personal confidential data".
Who requires access to the shared personal data?	You should employ 'need to know' principles, meaning that when sharing both internally between departments and externally with other organisations, individuals should only have access to your data if they need it to do their job, and that only relevant staff should have access to the data. This should also

	address any necessary restrictions on onward sharing of data with third parties.
When should it be shared?	Again, it is good practice to document this, for example setting out whether the sharing should be an on-going, routine process or whether it should only take place in response to particular events.
How should it be shared?	This involves addressing the security surrounding the transmission or accessing of the data and establishing common rules for its security.
How can we check the sharing is achieving its objectives?	You will need to judge whether it is still appropriate and confirm that the safeguards still match the risks.
How will individuals be made aware of the information sharing?	Have individuals been provided with the fair processing information as required by the Data Protection (Jersey) Law 2018? How is it ensured that individual's rights are respected and can be exercised e.g. how can they access the information held once shared?
What risk to the individual and/or the organisation does the data sharing pose?	For example, is any individual likely to be damaged by it? Is any individual likely to object? Might it undermine individuals' trust in the organisations that keep records about them?
What is the legal basis for data protection purposes?	Organisations must identify the lawful basis (e.g. meeting statutory duties) for processing and, where necessary, a condition for processing special categories data (e.g. managing a health and care service).
If the information is confidential	What is the legal basis that complies with the common law duty of confidence? This can be consent (implied or explicit), overriding public interest or required or permitted by law.

It is good practice to document all decisions and reasoning related to the information sharing. See Appendix 2 for an Information/Data Sharing Decision template.

If in any doubt about when it is appropriate to share information, staff should seek guidance from their Line Manager, Head of Information Governance & Systems or the Director of Governance & Care.

4 CONSULTATION PROCESS

Name	Title	Date
Claire White	Director of Governance & Care	2/10/2022
Mo De Gruchy	Quality and Performance Development Nurse	31/08/2022
Tia Hall	Operational Lead Adult Nursing	2/10/2022
Clare Stewart	Operational / Clinical Lead Out of Hospital Services	2/10/2022
Michelle Cumming	Operational Lead Child and Family Services	2/10/2022
Elspeth Snowie	Clinical Effectiveness Facilitator	2/10/2022
Elaine Walsh	Director of Finance	2/10/2022
Jenny Querns	Safeguarding Lead Nurse for Children & Adults	2/10/2022
Justine Bell	Education Lead and Practice Development Nurse	2/10/2022
Teri O'Connor	Home Care Manager	2/10/2022

5 IMPLEMENTATION PLAN

Action	Responsible Person	Planned timeline
Email to all staff	Secretary/Administration Assistant (Quality and Governance Team)	Within 2 weeks following ratification
Policy to be placed on organisation's Procedural Document Library	Secretary/Administration Assistant (Quality and Governance Team)	Within 2 weeks following ratification

6 MONITORING COMPLIANCE

The Head of Information Governance & Systems will monitor compliance with this policy and procedures, using internal audit reviews where necessary. Line Managers should also monitor compliance within their service areas. Related incidents reported on Assure can be used as a learning resource.

7 EQUALITY IMPACT STATEMENT

Family Nursing & Home Care is committed to ensuring that, as far as is reasonably practicable, the way services are provided to the public and the way staff are treated reflects their individual needs and does not discriminate against individuals or groups on any grounds.

This policy document forms part of a commitment to create a positive culture of respect for all individuals including staff, patients, their families and carers as well as community partners. The intention is to identify, remove or minimise discriminatory practice in the areas of race, disability, gender, sexual orientation, age and 'religion, belief, faith and spirituality' as well as to promote positive practice and value the diversity of all individuals and communities.

The Family Nursing & Home Care values underpin everything done in the name of the organisation. They are manifest in the behaviours employees display. The organisation is committed to promoting a culture founded on these values.

Always:

- ✓ Putting patients first
- ✓ Keeping people safe
- ✓ Have courage and commitment to do the right thing
- ✓ Be accountable, take responsibility and own your actions
- ✓ Listen actively
- ✓ Check for understanding when you communicate
- ✓ Be respectful and treat people with dignity
- ✓ Work as a team

This policy should be read and implemented with the Organisational Values in mind at all times.

8 GLOSSARY OF TERMS

Anonymous Data means Personal Data that has been processed in such a manner that it can no longer be attributed to an identified or identifiable natural person.

Personal Data - Any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of that natural person.

Special Category Data - Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; Genetic or biometric data that is processed for the purpose of uniquely identifying a natural person; Data concerning health; Data concerning a person's sex life or orientation; Data relating to a person's criminal record or alleged criminal activity

9 REFERENCES

Caldicott Committee (1997) *Report on the Review of Patient-Identifiable Information.* Department of Health, London

Department of Health (2013) *Information: To Share or not to Share.* Available at: Information: To Share or not to Share (publishing.service.gov.uk). Last accessed 31st August 2022

Information Commissioners Office Data sharing information hub | ICO

Information Commissioners Office (2021) *Introduction to Anonymisation.* Available at anonymisation-intro-and-first-chapter.pdf (ico.org.uk). Last accessed 31st August 2022

Jersey Care Commission (2019) *Jersey Care Commission Standards for Home Care.* Available at JCC-Care-Standards-Home-Care-2019-v1..pdf (carecommission.je). Last accessed 18th March 2022

States of Jersey (2011) *Freedom of Information (Jersey) Law.* Available at Freedom of Information (Jersey) Law 2011 (jerseylaw.je). Last accessed 25th March 2022.

States of Jersey (2018) *Data Protection (Jersey) Law.* Available at DATA PROTECTION (JERSEY) LAW 2018 (jerseylaw.je). Last accessed 18th March 2022

UK Caldicott Guardian Council (2021) *The Common Law Duty of Confidentiality.* Available at Duty of confidentiality — UKCGC. Last accessed 28th October 2021

Children and Young People (Jersey) Law 2022 (jerseylaw.je)

10 APPENDIX

Appendix 1 Equality Impact Screening Tool

Stage 1 - Screening			
Title of Procedural Document: Information Sharing Policy			
Date of Assessment	16/08/2022	Responsible Department	Governance
Name of person completing assessment	Claire Whelan	Job Title	Head of Information Governance & Systems

Does the policy/function affect one group less or more favourably than another on the basis of :		
	Yes/No	**Comments**
• Age	No	
• Disability Learning disability; physical disability; sensory impairment and/or mental health problems e.g. dementia	No	
• Ethnic Origin (including hard to reach groups)	No	
• Gender reassignment	No	
• Pregnancy or Maternity	No	
• Race	No	
• Sex	No	
• Religion and Belief	No	
• Sexual Orientation	No	
If the answer to all of the above questions is NO, the EIA is complete. If YES, a full impact assessment is required: go on to stage 2, page 2		

Stage 2 – Full Impact Assessment			
What is the impact	**Level of Impact**	**Mitigating Actions** (what needs to be done to minimise / remove the impact)	**Responsible Officer**

Monitoring of Actions
The monitoring of actions to mitigate any impact will be undertaken at the appropriate level

Appendix 2 Information/Data Sharing Decision template

For recording Caldicott Guardian queries / advice / information sharing decisions

What pieces of law have been considered? (e.g. Data Protection Act, Common Law etc)

What professional guidance has been considered? (e.g. NMC)

How have the Caldicott Principles been considered and satisfied?

1. Justify the purpose (s)
2. Don't use personal confidential data unless it is absolutely necessary
3. Use the minimum necessary personal confidential data
4. Access to personal confidential data should be on a strict need-to-know basis
5. Everyone with access to personal confidential data should be aware of their responsibilities
6. Comply with the law
7. The duty to share information for individual care is as important as the duty to protect patient confidentiality
8. Inform patients and service users about how their confidential information is used

Who have I talked to? (Including professionals, sources of advice, the individual or their relatives)

Is the information presented sufficient to make a decision or is more needed? Is urgency a factor?

What is the rationale for the decision? (How are the different factors involved being considered)

What is the decision?
(Including: how it is to be implemented & whether it has been shared with the individual(s))
