The Walton Centre NHS Foundation Trust

Excellence in Neuroscience

Data Sharing Agreement Policy

Author and Contact details:	**Information Governance Manager** **Tel:** **Email:**	
Responsible Director:	**Director of Finance**	
Approved by and date:	**Information Governance Security Forum**	**October 2015**
Document Type:	**POLICY**	**Version 2.0**
Target Audience:	All trust employees.	
Document Approval, History/Changes	**See Appendix 3** For further information contact the Governance Department on **Tel:**	

Think of the environment…Do you have to print this out this document? **You can always view the most up to date version electronically on the Trust intranet.**

Executive Summary

This Data Sharing policy outlines the process to be followed between organisations that need to share person identifiable information. It sets out the obligations and commitments that staff must follow to ensure that legislation is not breached and patients' / clients' / families' / carers' / staff / employees' (collectively referred to as "service users" throughout this document) confidentiality is maintained.

Contents

1. Introduction

This policy outlines national and the Walton Centre NHS Foundation Trust standards for information sharing. Further advice on any aspect of the enclosed policy can be gained from the Information Governance Department.

This Data Sharing policy outlines the process to be followed between organisations that need to share person identifiable information in all formats. It sets out the obligations and commitments that staff must follow to ensure that legislation is not breached and patients' / clients' / families' / carers' / staff / employees' (collectively referred to as "service users" throughout this document) confidentiality is maintained.

An overarching principle of this Agreement is that each organisation must have signed up to the IG SoC (Statement of Compliance). This provides confidence that all organisations will have in place or be working towards the security standards required by the Health and Social Care Information Centre.

Participant organisations will process personal data (as the term 'personal data' is defined in section 1(1) of the Data Protection Act 1998) in accordance with the Data Protection Act 1998 and, will maintain in place, having regard to the state of technological development and the cost of implementation, all appropriate measures, procedures and policies to protect the security and integrity of any such personal data. The policy and procedural control mechanisms detailed within this Agreement augment those already implemented in accordance with the IG SoC.

This policy outlines the principles of confidentiality and establishes an interagency code of practice with regard to the confidential management of service user's information.

Information sharing protocols are used as a useful way of providing a transparent and level playing field for organisations that need to exchange information. They provide assurance in respect of the standards that each party to an agreement will adopt. However, they do not in themselves provide a lawful basis for sharing confidential information. That can only result from effectively informing the person whose information it is about the possibility of sharing and the choices they have to limit sharing. If the individual says no to sharing, then confidential information may only be shared in exceptional circumstances and in line with the Data Protection Act 1998. It is consent that determines whether information can be shared – with consent you don't need an information sharing agreement for sharing to be lawful, without it an agreement is of no help.

1.1. Objectives of the Policy

The objectives of this policy are:

- To provide a framework to clarify local procedures relating to the sharing of service user information;
- To ensure everyone working with personal information understands the importance of information sharing, where it improves care for service users and it is for the direct continuing care of service users;
- To ensure that only the minimum information necessary for the purpose should be shared;
- To ensure that when information needs to be shared, that sharing complies with the law, guidance and best practice;
- To ensure that service users' rights are respected;

- To ensure that confidentiality is adhered to unless there is a robust public interest in disclosure or a legal justification to do so;
- To outline the importance and benefits of information security and confidentiality training;
- To provide a mechanism for signatories to this policy to agree that their organisation and staff will comply with the standards and best practice for information sharing contained within this policy;
- To establish mechanisms for monitoring and audit of this policy.

2. Scope

This policy covers all aspects of information sharing within the organisation, including (but not limited to):

- Patient/Client/Service User information
- Staff related information
- Organisational information

3. Definitions

3.1. Information Sharing Partners

Organisations will need to share confidential person-identifiable information with a range of others. The purposes of sharing information will either relate to the provision of care, including the quality assurance of that care, for the individual concerned or will be for non-care or secondary purposes, e.g. service evaluation, research, finance, public health work etc.

Information partners will cover a range of organisation types, some of which will be 'trusted' organisations, whilst others will not. Organisations that can demonstrate they are attaining an acceptable level of information governance (IG) performance are those that are meeting the NHS Operating Framework key requirements. Some organisations are mandated to carry out IG assessments and ensure they reach an acceptable standard, such as:

- NHS organisations;
- Commissioning Support Unit (CSU)
- Clinical Commissioning Group (CCG)

Others have a requirement to meet the key requirements because they are working with or for NHS organisations or have access to national NHS services and systems. This group will include some (but not all of) organisations such as:

- Adult social care services;
- Voluntary sector providers;
- Private sector care providers;
- Hospices;

Information sharing partners will also include organisations that have no current requirement to carry out IG assessments or do not provide IG assurance in the same way, such as:

- The police;
- District and borough councils;
- Sure start teams;
- Education services;
- Housing services;

- Research organisations;
- The Department for Work and Pensions;
- Fire and rescue services;
- Youth offending teams;
- Court services;
- Probation services;
- The Crown Prosecution Service.

3.2. Sharing for non-care purposes

The approach where confidential personal information needs to be shared for non-care purposes needs to be managed somewhat differently even where the sharing is with a 'trusted' organisation. This is because the purposes for sharing need to be defined and limited, and additional requirements such as recorded informed consent or evidence of support under section 251 of the NHS Act 2006 (formerly section 60 of the Health & Social Care Act 2001), may be required to enable lawful sharing.

With 'trusted' organisations the required information sharing protocol only needs to focus on those aspects of sharing – purpose, constraints on re-use of information, retention periods and destruction policies – that are not normally associated with sharing for care purposes.

With other organisations, e.g. research or other secondary use organisations, the protocols will need to address both the basic information governance standards that should apply and the additional ones associated with the secondary uses in question – i.e. purpose, constraints on re-use of information, retention periods and destruction policies.

4. Duties

4.1. Chief Executive

The Chief Executive has overall responsibility for information sharing in the Trust. As the chief accountable officer he is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Information Sharing is the key to this as it will ensure appropriate, accurate information is available as required.

4.2. Caldicott Guardian

The Trust's Caldicott Guardian has a particular responsibility for reflecting patients' interests regarding the use of patient identifiable information. They are responsible for ensuring patient identifiable information is shared in an appropriate and secure manner. The Caldicott Guardian is the Trust's Medical Director.

4.3. Senior Information Risk Owner (SIRO)

The SIRO (Senior Information Risk Owner) has responsibility for ensuring that organisational information risk is properly identified, managed and that appropriate assurance mechanisms exist. The SIRO should:

- Lead and foster a culture that values, protects and uses information for the success of the organisation and benefit of its customers;
- Own the organisation's overall information risk policy and risk assessment processes and ensure they are implemented consistently;
- Advise on the management of information risk and provide assurance;
- Own the organisation's information incident management framework.

The Walton Centre's SIRO is the Director of Finance.

4.4. Information Governance Security Forum (IGSF)

The IGSF is responsible for ensuring that this policy is implemented, and that the information sharing systems and processes are developed, coordinated and monitored. The Trusts Caldicott Guardian and designated officer is responsible for the overall development and maintenance of information sharing practices throughout the Trust, in particular for drawing up guidance for good information sharing practice and promoting compliance with this policy in such a way as to ensure the easy, appropriate and timely sharing of information. The IGSF will monitor implementation of and adherence to this policy. Breaches of confidentiality will be a standing agenda item for the IGSF and this will include all incidents relating to information sharing.

4.5. Designated officer (IG Manager)

To comply with the overarching information sharing protocol the Trust has a designated officer to oversee the information sharing process on behalf of the Caldicott guardian.

1. Produce clear policies to enable staff to access the designated officer.
2. Designated officer should endeavour to make collective decisions and to document the arguments in support or against those decisions
3. Designated officer will be encouraged to bring examples of difficult decisions or dilemmas to the information governance for peer support and evaluation
4. Designated officer should be fully aware of their duties and obligations under relevant legislation
5. Requests for information should be made to the designated officer in writing
6. Written records of disclosure requests, disclosure decisions and the details of the information disclosed should be made and kept. The data owner should always be recorded.
7. The IGSF will review decisions that have been taken with the Caldicott guardian for the Walton Centre NHS Foundation Trust.
8. With respect to information sharing requests and disclosures the designated officer will be responsible for:
    - Liaising with the Caldicott Guardian for Caldicott issues;
    - Ensuring the confidentiality of information at all stages;
    - Ensuring the security of information at all times;
    - Ensuring compliance with legislation;
    - Ensuring that a request or disclosure is legal and common law provisions permitting disclosure are adhered to;
    - Checking with the partner or agency named that the exchange is necessary to fulfil a clearly specified role or objective that is covered by the information sharing protocol;
    - Checking that the terms and conditions of the information sharing protocol are followed;
    - Making or approving a request for information in writing:
    - Controlling the release of information;
    - Ensuring that any data exchanged is accurate;
    - Ensuring information is only sent or received by an authorized individual or agency;
    - When necessary, providing written consent for a secondary disclosure of information originally held by them to a third party;
    - Auditing and monitoring exchanges;
    - Dealing with complaints related to this process.

4.6. Local Managers

The responsibility for local information sharing is devolved to the relevant directors and managers, heads of departments and business functions within The Walton Centre have overall responsibility for information sharing generated by their activities, i.e. for ensuring that information is shared in an appropriate and timely manner and in a way which meets the aims of this policy.

4.7. All staff

All Walton Centre NHS Foundation Trust whether clinical or administrative, who share information have information sharing responsibilities. In particular all staff must ensure that they only share information in an appropriate and timely manner in accordance with this policy and any guidance subsequently produced. All staff have a confidentiality clause within their contract of employment. All staff must complete mandatory information governance training. There will be disciplinary sanctions for failure to comply with duties which may result in dismissal or bringing criminal charges.

5. Process

The Walton Centre NHS Foundation Trust has signed up to the Information Sharing Code of Practice. This Overarching Standard for Information Sharing is designed to be used in conjunction with a set of documents within a Tiered Structure. The structure is designed to provide a framework for the secure and confidential sharing of information between the partner organisations that contribute to the wellbeing of residents and ensuring disclosure is in line with statutory requirements.

There are 3 main tiers to the structure:

Tier Zero- This is a document signed by the Chief Executive of the Walton Centre NHS Foundation Trust agreeing in principle to share information responsibly.

Tier One- This is an overarching standard outlining the agreed procedures for sharing information. It is this document which sets the standards for obtaining, recording, holding, using and sharing of information and outlines the supporting legislation, guidelines and documents which govern information sharing between partner organisations

Tier Two- This gives guidance to all operational staff on the production of a protocol for the safe sharing of information. These protocols should show what information should be shared and how, under what circumstances and by whom, and should be tailored to individual partnerships. This document will require authorisation of the participating partnership organisations.

This Code of Practice has been designed to simplify and strengthen the sharing of information between partner organisations.

The Tier 2 document in Appendix 1 must be used in all cases when setting up a new Data Sharing Agreement with another organisation.

The questions in Appendix 2 must be answered in all instances.

Completed Data Sharing Agreements must be logged with the Information Governance Department for review and for their records.

The Information Governance Department will liaise with the IGSF & the Caldicott Guardian for sign off.

6. Training

The policy & supporting guidance will be made available to all staff on the Trust's intranet and will be reviewed through the Information Governance and Security Forum and then ratified at Business Performance Committee The intent set out within this policy is applicable across the Walton Centre Foundation Trust and contains sufficient detail to ensure consistency across the Trust's full range of business environments and functions.

7. Monitoring

The policy's effectiveness will be monitored and reviewed periodically through the Trust's Information Governance and Security Forum and the Trust Board.

8. References

- Access to Health Records Act 1990 (only for manual records of deceased patients)
- Audit Commission Act 1998
- Children's Act 1989
- Common Law Duty of Confidence
- Computer Misuse Act 1990
- Data Protection Act 1998
- Freedom of Information Act 2000
- Health & Social Care Act 2001
- Human Rights Act 1998

8.1. Supporting policies/documents

This policy should be read in conjunction with the following policies and guidance which are available on the Trust's intranet.

- Information Governance Policy
- Information Governance & Security Forum Terms of Reference
- Data Protection Policy
- Code of Conduct for Employees in Respect of Confidentiality
- Clinical Records Management Policy
- Lifecycle Management Strategy
- Freedom of Information Policy

Appendix 1 - Data Sharing Agreement (Tier 2)

Appendix 2 - Checklist for Information Sharing

(To be read in conjunction with Data Sharing Tier 2 Document)

Paragraph number	Question	Answer
3a	Who are the organisations who are party to the agreement?	
3b	Why do you want to share? What is the Purpose of Information Sharing? Does the purpose comply with the Data Protection Act and other key legislation listed in Tier 1	
3c	What will the benefits of sharing be?	
3e	Are there Statutory duties to share this information? Is it a partnership as a direct result of legislation or a government initiative? Are there any restrictions on sharing this information? Legal, commercial.	
3f	What information do you need to share? Is confidential or sensitive information to be shared? List specifically what data is intended to be shared	
3g	Are there any alternatives to sharing personal information? Can the information be anonymised?	

Paragraph number	Question	Answer
3h	What are the consequences of not sharing information?	
3i	Who will be affected by the agreement? e.g. Children, older people, people living in a particular area, specific groups What are the risks in sharing the information? Is any individual likely to be damaged or harmed by information being shared? Is any individual likely to object?	
3j	What new processes or procedures will be required to enable information to be shared? Will new or changed authentication checks be required that could be intrusive? i.e. How will the information be obtained, who will access, when access necessary, audit trails, physical security and system security. How will staff be trained in using the new process/procedure? The procedures could be attached to the completed Tier 2 document or reference made to where they will be held.	
3k	Are outside contractors to be used? Contracts need to include confidentiality clause re Information Governance Security requirements.	

Paragraph number	Question	Answer
4	How will the public be informed that their information will be shared?	
	The public need to be told:	
a	What information will be shared?	
b	Who with, which staff/organisation will see it?	
c	When will information be shared?	
d	Is a Fair Processing Notice required?	
e	How will you distribute the fair processing information?	
f	Do the public know who to contact for enquiries?	
g	How will consent be obtained to share the information?	
h	What procedures will be in place to allow sharing without consent? Include risk assessments, documentation of decision	
5a	What quality assurance checks are in place to ensure recorded information is of an acceptable quality?	
b	When will information be recorded, who will record the information?	
c	Is the information collected relevant? Will all the information be needed?	
d	How will the quality of the information be reviewed?	

Paragraph number	Question	Answer
e	Who will be the data controller?	
6a b c d e f	What retention period has been agreed for the information? What is the review period for the retention policy? What are the legal requirements to retain or delete information? Will the information be archived or deleted when no longer required? How will this be done? Who will be responsible for holding the information? (The Information Asset Owner for the information) Who will be responsible for ensuring each organisation complies with the agreed retention policy and how will this be done?	
7 a b c	Who will be responsible for security of the system holding the information? Who will monitor access to the system and report breaches/incidents? What process is in place to deal with incidents/breaches or staff non-compliance with procedures? Who will be responsible for technical security? (user access – issue of passwords, system restrictions, backup procedures for system) Is there organisational security in place to prevent access to	

Paragraph number	Question	Answer
d	offices, fax machines, computers or areas where personal information may be seen by the public? Who is the data controller for the information? Need to agree responsibilities of each organisation and document.	
8	Who will process Subject Access Requests and how will this be done? Subject Access Request = where service users have requested to see their personal information i.e. Which organisation will process Subject Access Requests? Do the public know how they can access their information?	
9	What review period has been agreed for the Information Sharing protocol? Need to check that the sharing of information is still achieving its objectives, still appropriate and the safeguards still meet the risks. Who will undertake the review?	
10	What is the process for dealing with complaints from service users? Who will process them? How will they be reported to partner organisations?	

Paragraph number	Question	Answer
11	Detail process for resolution of a dispute between partner organisations. Nominated officers for dealing with dispute, Investigations, findings, remedial action, consequences, notification of affected service users and organisation.	
12	Include a list of lead officers involved in agreeing this Information Sharing Protocol. Obtain signatures from lead officers when they have agreed and ensure copies of signed Information Sharing Protocol given to all parties including the Information Governance Team for the organisation.	

Appendix 3 - Version Control

Version	Section/Para/ Appendix	Version/description of amendments	Date	Author/Amended by
1.0	-	New Document	17/02/2014	IG Manager
2.0	Appendix 2	Insertion of new template	24.07.2015	Deputy IG Manager

Translation Service

This information can be translated on request or if preferred an interpreter can be arranged. For additional information regarding these services please contact The Walton centre on 0151 525 3611

Gellir gofyn am gael cyfieithiad o'r deunydd hwn neu gellir trefnu cyfieithydd ar y pryd os yw hynny'n well gennych. I wybod rhagor am y gwasanaethau hyn cysylltwch â chanolfan Walton ar 0151 525 3611.

هذه المعلومات يمكن أن تُتَرْجَم عند الطّلب أو إذا فضّل المترجم يمكن أن يُرَتَّب للمعلومة الإضافيّة بخصوص هذه الخدمات من فضلك اتّصل بالمركز ولتون على 0151 5253611

ئەم زانیاریە دەکرێت وەربگێڕدرێت کاتێك کە داواکرێت یان ئەگەر بەباش زانرا دەکرێت وەرگێڕێك ئامادە بکرێت (ڕێك بخرێت) ، بۆ زانیاری زیاتر دەربارەی ئەم خزمەتگوزاریانە تکایە پەیوەندی بکە بە Walton Centre بە ژمارە تەلەفۆنی ١٥١٥٢٥٣٦١١ .

一经要求，可对此信息进行翻译，或者如果愿意的话，可以安排口译员。如需这些服务的额外信息，请联络Walton中心，电话是：0151 525 3611。