The Tavistock and Portman NHS
NHS Foundation Trust

Data Sharing Procedure

Version:	1.1
Bodies consulted:	Caldicott Guardian
Approved by:	PASC
Date Approved:	24.4.15
Name of originator/ author:	S.I Ndumbe
Lead Director:	SIRO
Date issued:	Apr 15
Review date:	Mar 21

Contents

Data Sharing Procedure

1 Introduction

The procedure sets out how the Trust discharges its obligations in relation to sharing data. In this context, sharing means the transmission of personal data between one or more parties, rather than in the sense of *disclosing* information and managing confidentiality in therapy or training.

Whilst it may seem perfectly obvious to staff why data is collected and shared, it may not be obvious to service users. This procedure sets out what factors need to be considered before deciding to share information, how sharing can be undertaken safely, and what service users should be told.

While confidentiality is very important, as is the duty to share information: each situation must be judged on its merits and advice should be sought as required.

2 Purpose

The Data Sharing Code of Practice (2011) (the Code) is issued by the Information Commissioner's Office (ICO) and is a statutory code of practice and is established under the Data Protection Legislation. This procedure sets out how the Trust will implement the ICO's Code.

3 Scope

Any data sharing, internal or external, in any media, by whatever means, regardless of scale or content, is covered by this procedure. This procedure sets out how the Code will be implemented and audited; it is not intended as an interpretation: staff must follow the Code's directions and refer to the Code when considering how best to transact exceptional requests, that is, those not covered by established agreements and processes.

4 Definitions

Personal Data	Data that include personal identifiable information
Sensitive data	Personal data that include personal health, ethnic origin/race, religious, trades' union, sexual, or criminal record information.
Data subject	An individual to whom data refers
Systematic sharing	Routine sharing for an agreed purpose
Exceptional sharing	Sharing not covered by pre-established agreements.
Data control	Determining the purpose and/or manner for/of data processing
Data processing	Handling or holding data for any purpose, not necessarily manipulating the data.

5 Duties and responsibilities

Director of Transformation and Technology
Is accountable to the Director of Finance for the Informatics and ICT teams.

Director of Quality and Patient Experience
Is accountable to the Chief Executive for clinical data quality.

Senior Information Risk Owner (SIRO)
Reports to the Trust Board and is accountable of the Trust information risk management

Information Governance Manager and DPO
Reports to the SIRO and in is accountable of the Trust information governance and is the Trust's lead on data protection.

Informatics Manager

Reports the Trust Director of Transformation and Technology and is accountable of the Trust Informatics Department, and Clinical and student systems.

Information Technology Manager
Is reports to the Director of Transformation and Technology and accountable of the IT Department

Caldicott Guardian
Can be called on for impartial advice on whether data *should* be shared, especially where clinical ethics are being considered.

Directors
Are responsible for ensuring that information assets and data flows in their directorates are managed according to Trust procedures

Clinical staff
It is the responsibility of the lead clinician to discuss data sharing in the clinical context and record consent thereto.

All Staff
Staff must ensure that their practice is safe and complies with the Trust policies, professional codes of conduct, and contractual requirements.

6 Procedures

a) Deciding to share data

i) Consent

The Trust processes personal data, including sensitive personal data; consent to handle such data is a part of the process of engagement with the data subject, eg when the clinician obtains consent for treatment, or when a student joins an education or training programme. However, consent to process data as part of a treatment or education programme does not necessarily give consent to share data, specific and separate consent to share needs to be obtained (though in practice this can of course be obtained as part of one consent 'exercise').

ii) Factors to consider

The Code sets out some factors to consider before deciding to share data, eg:

- What would sharing achieve?
- What needs to be shared?
- Would anonymised data be sufficient instead?
- Who needs to know?
- When should it be shared?
- What are the risks?
- How will effectiveness of the sharing be assessed?

Extra care must be taken when handling sensitive data, eg all patient records and personnel files; consent or explicit consent is likely to be needed when:

- Information is going to be shared without a clear legal basis
- The individual is likely to object
- Sharing would have a significant effect on an individual or group.

In everyday practice, systematic data sharing agreements are usually already in place, eg for patients the type of information shared and with whom is set out in the patient leaflet *'Your personal information and how it is used'* ; for students, the course handbooks make clear that information is shared with university partners for the purposes of making awards.

iii) Establishing routine arrangements

For most activity, data will be shared in order to expedite Trust business and data sharing agreements will be in place to set out the various controls needed. The Trust's privacy notice outlines the situations when this would occur. All known arrangements are logged on the Trust's Information Asset Register. Staff wishing to establish a new data sharing arrangement should complete the checklist in appendix B and refer to the Governance Manager.

iv) *Ad hoc* arrangements

These will be exceptional, and typically will involve people at risk. Professional codes of conduct should be consulted. Staff wishing to establish a new data sharing arrangement should complete the checklist in appendix C and refer to the Governance Manager.

v) Objections to data sharing by data subjects

All such requests must be responded to within 21 days. The request need not necessarily be accepted and it may be appropriate to discuss the objection in order to ally unfounded concerns. If a request is agreed, then the requestor must be informed that it has been done/ will be done. In any case, advice should be sought from the Information Governance Manager/DPO or Caldicott Guardian in the first instance.

b) Telling people about sharing their data

i) Patients

- Patients have a right to expect that information about them will be kept confidential by employees of the NHS (Confidentiality: NHS Code of Practice 2010).
- Staff have a duty to share information, and this duty is of equal importance with the duty of confidentiality.
- Staff must have the appropriate authority before sharing patient identifiable patient information.

- If a patient is unable to consent to the sharing of their personal information the clinician must abide by the requirements of the Mental Capacity Act 2005.

i) Disclosing personal information with patient consent

Personal information about patients will be shared for the purposes of supporting the delivery of their care (considering the factors in a (ii) above)

Patients have a legal right to information held about them and staff should work on the presumption that all they write and share be seen by the patient.

The wishes of a patient who objects to particular personal information being shared within healthcare/with others must be respected unless disclosure would be justified in the public interest.

ii) Disclosing personal information where patient lacks capacity to consent to sharing.

Note: Staff should understand the principles of the Mental Capacity Act 2005 and seek advice on assessing a patient's mental capacity and understanding.

When deciding to share information about a patient who lacks capacity the clinician should support and encourage the patient to be involved in sharing of their personal information as far as they want and are able.

The clinician must consider whether the patient's lack of capacity is permanent or temporary and if the decision to disclose could reasonably be deferred until patient regains capacity.

The clinician must consider any evidence of the patient's previously expressed preferences and the views of anyone who has legal authority to make decision on behalf of patient/legally appointed as representative or anyone the patient has indicated should be consulted.

The clinician must consider the views of people close to the patient about the patient's likely preferences and whether they consider the proposed sharing to be in the best interests of the patient.

If any member of staff believes that a patient may be a victim of neglect or physical, sexual or emotional abuse, where the patient lacks capacity to consent to sharing, they must act in the patient's best

interests and share information (please refer to Safeguarding Vulnerable Adults Procedure).

iii) Disclosing personal information to carers where patient lacks capacity to sharing information

Unless a patient has indicated otherwise it is reasonable to assume that he/she would want those closest to them to be kept informed of their general condition and prognosis.

It may be necessary to share personal information with a patient's relatives, or carers in order to make an assessment or devise a treatment plan.

If possible, establish with the patient what information they want to share, with whom, and in what circumstances. This is particularly important if the patient's capacity is fluctuating or if patient is likely to lose capacity, even if this is a temporary loss.

Clinicians must share relevant information to an appropriate person (relative/carer/authority) if this is in the patient's best interests.

Sharing personal information with a relative/carer does not mean that they then have a general right of access to the patient's medical records.

iv) Staff

The Trust does not normally share personal Identifiable staff data with third parties (but see section c). For routine monitoring and business purposes, the Trust will ensure that data is anonymised.

v) Other service users

The Trust does not normally share personal identifiable student or consultancy client data with third parties. For students there are times when it is necessary and justified to do so:-

Local Authorities

In order to administer exemptions of properties from council tax students' personal data will be shared with the relevant local authority from which the exemption is being sought.

Higher Education Statistics Agency (HESA), HE funding councils and other government bodies

Students' personal data will be provided to HE funding councils, government bodies and HESA. Further details about the data shared with HESA can be found in the HESA-Student collection notice on the HESA website.

Higher Education Academy

The Trust is required to pass data to the Higher Education Academy as part of participation in the Post-graduate Research Experience Survey. This survey students the chance to give feedback on their experiences at the Trust and so informing the choices of prospective students. It is described in detail on the Higher Education Academy website.

The Trust will pass names and contact details to the agent carrying out the survey. The agent may then invite students to take part. Students do not have to take part in the survey and can opt out at any time by contacting the agent and providing them with verification of their identity by confirming their date of birth.

Higher Education (HE) institutions
Where students are involved in award programmes validated by a University Partner organisation, the Trust may disclose their personal data for general educational and assessment purposes.

Sponsors, loan organisations and scholarship schemes
Personal data about students may be disclosed to third parties attempting to recover debt on behalf of the Trust where internal procedures have failed.

Parents, guardians and other relatives
Other than in the most exceptional of circumstances, the Trust will not to disclose a student's personal data to parents, guardians and any other relative. If students have provided a nominated contact in the event of a medical problem or emergency then some personal data may be provided.

Published information
Examination results and any award (such as a degree) made by the Trust and University Partner organisation is a matter of public record rather than personal data, and as such will be publicly available and publicised at, for instance, graduation ceremonies.

Photographs of students during the course of their study may also be taken. If you do not wish your photograph to be taken, then simply absent yourself from any pictures. Group photographs taken will assume the permission of individuals pictured for use in Trust publications and publicity materials, and publications produced by third parties authorised by the Trust. Attendance at graduation ceremonies will assume the permission of the attendees and photographs and recordings taken one the day may be publicised on the Trust's and University Partner organisation's website.

In most cases, external requests regarding students should be sent to the Associate Director of Education & Training and external requests regarding consultancy clients to the Director of Tavistock Consulting.

c) Not telling people about sharing their data

The Trust is legally required to share information in certain circumstance, and this may include occasions in which information can be shared without consent, for example:-

- The prevention and detection of crime
- The apprehension and prosecution of offenders
- The assessment of tax and duty

In these cases, data can, and possibly must, be shared without consent or knowledge of the service user.

d) Safe practice

Whether data is shared internally or externally the following should be taken into consideration:-

- There must be a legitimate purpose –see Data Protection Procedure
- Whether consent is needed
- The Caldicott Principles will always apply to patient data
- Either the Health records Procedure will apply, or the Corporate Records will apply to all records handled by the Trust
- Electronic transfer must be effected using the email procedure (which specifies, among other matters, the addresses which can safely be used)
- Additional procedures also apply, eg Information Communication Technology Security Procedure
- Check for accuracy before sharing data
- Ensure corrections made to duplicate sets are made to each and every set
- Notify the receiving party of the requirements of the Trust's Retention Schedule, and of their obligation not to retain data for longer than is allowed by this Schedule

The relevant appendix[1] B or C should be completed in order to clarify a sharing arrangement, unless the arrangement is part of the routine management of an information asset for which a Privacy Impact Assessment has been completed.

[1] A Word version of this for is available from the Governance Manager

e) Things to avoid

- Misleading individuals so as to avoid possible objections
- Sharing irrelevant or excessive data
- not checking accuracy before sharing
- use of incompatible systems, thus compromising the data
- not following related Trust procedures.

7 Training Requirements

All staff shall undertake basic Data Security and Protection (IGT) training on an annual basis, certain staff will undertake additional training on data handling as directed by the SIRO or IG Manager/DPO.

8 Process for monitoring compliance with this Procedure

The Information Governance Manager and DPO or Director or Transformation and Technology will report the management of all information assets to the IG Work Stream of the Clinical Quality Safety and Governance Committee of the Board of Directors.

9 References

Guidance:-
http://www.ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Detailed_specialist_guides/data_sharing_code_of_practice.ashx

Checklists:-
http://www.ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Practical_application/data_sharing_checklists.ashx

Confidentiality: NHS Code of Practice 2010

Safeguarding Vulnerable Adults Procedure.

10 Associated documents[2]

Guidelines for using patient information

[2] For the current version of Trust procedures, please refer to the intranet.

Data Protection Procedure
e-mail and internet use procedure.
Information Communication Technology Security Procedure
Retention Schedule
Consent to Treatment Policy and Procedure
Privacy Notice

Appendix A : Equality Impact Assessment

1. Does this Procedure, function or service development affect patients, staff and/or the public?

YES

2. Is there reason to believe that the Procedure, function or service development could have an adverse impact on a particular group or groups?

NO

*3. If you answered **YES in section 2,** how have you reached that conclusion? (Please refer to the information you collected e.g., relevant research and reports, local monitoring data, results of consultations exercises, demographic data, professional knowledge and experience)*

4. Based on the initial screening process, now rate the level of impact on equality groups of the Procedure, function or service development:

Negative / Adverse impact:

Low…….

Positive impact:

Low……..

Date completed: 26.7.13

Date reviewed: 10.05.2018

Name: S.I Ndumbe

Job Title: Information & Secuirty Governance Manager and DPO

Appendix B : Data sharing checklist – establishing routine arrangements

Scenario: You want to enter into an agreement to share personal data on an on-going basis

Is the sharing justified? Key points to consider:	**Do you have the power to share?** Key points to consider:	**If you decide to share…** It is good practice to have a data sharing agreement in place. As well as considering the key points above, your data sharing agreement should cover the following issues:
What is the sharing meant to achieve?	The type of organisation you work for.	What information needs to be shared.
Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?	Any relevant functions or powers of your organisation.	The organisations that will be involved.
Is the sharing proportionate to the issue you are addressing?	The nature of the information you have been asked to share (for example was it given in confidence?).	What you need to tell people about the data sharing and how you will communicate that information.
Could the objective be achieved without sharing personal data?	Any legal obligation to share information (for example a statutory requirement or a court order).	Measures to ensure adequate security is in place to protect the data.
-	-	What arrangements need to be in place to provide individuals with access to their personal data if they request it.
-	-	Agreed common retention periods for the data.
-	-	Processes to ensure secure deletion takes place.

Record your decision Record your data sharing decision and your reasoning – • whether or not you shared the information. • If you share information you should record:	
What information is to be shared and for what purpose:	
With whom it will be shared:	
When it will be shared:	
Your justification for sharing:	
Whether the information is to be shared with or without consent:	
Name:	
Title:	
Date:	

For Office Use Only	
Received:	
Approved Y/N:	
By:	
Comments:	

Send completed form to the Information & Security Governance Manager and DPO

11 Appendix C : Data sharing checklist for *ad hoc* arrangements

Scenario: You are asked to share personal data relating to an individual in 'one off' circumstances

Is the sharing justified? Key points to consider:	**Do you have the power to share?** Key points to consider:	**If you decide to share…** Key points to consider:
Do you think you should share the information?	The type of organisation you work for.	What information do you need to share? – Only share what is necessary. – Distinguish fact from opinion.
Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?	Any relevant functions or powers of your organisation.	How should the information be shared? – Information must be shared securely. – Ensure you are giving information to the right person.
Do you have concerns that an individual is at risk of serious harm?	The nature of the information you have been asked to share (for example was it given in confidence?).	Consider whether it is appropriate/safe to inform the individual that you have shared their information.
Do you need to consider an exemption in the DPA to share?	Any legal obligation to share information (for example a statutory requirement or a court order).	-
Record your decision Record your data sharing decision and your reasoning – • whether or not you shared the information. • If you share information you should record:		

What information was shared and for what purpose:	
With whom it was shared:	
When it was shared:	
Your justification for sharing:	
Whether the information was shared with or without consent:	
Name:	
Title:	
Date:	
For Office Use Only	
Received:	
Approved Y/N:	
By:	
Comments:	

Send completed form to the Information & Secuirty Governance Manager and DPO