Tees, Esk and Wear Valleys NHS
NHS Foundation Trust

Leeds and York Partnership NHS
NHS Foundation Trust

Information Sharing Agreement

between

Leeds and York Partnership NHS Foundation Trust

and

Tees, Esk and Wear Valleys NHS Foundation Trust

for the

Eating Disorders and Forensic Services

Date effective from:	01/10/2013
Review date:	30/09/2015
Version number:	1.0

See Document Summary Sheet for full details

Tees, Esk and Wear Valleys NHS
NHS Foundation Trust

Leeds and York Partnership NHS
NHS Foundation Trust

DOCUMENT SUMMARY SHEET

ALL sections of this form must be completed.

Document title:	LYPFT & TEWV Eating Disorders and Forensic Service ISA
Document reference number:	ISA-0008
Version number:	1.0
Document author (Title)**:**	LYPFT: Information & Knowledge Manager TEWV: Information Governance and Records Manager
Document author (Name)**:**	LYPFT: Carl Starbuck TEWV: Louise Eastham
Ratified by:	LYPFT: Medical Director & Caldicott Guardian TEWV: Director of Nursing and Governance and Caldicott Guardian
Date ratified:	01/10/2013
Date effective from:	01/10/2013
Review date:	30/09/2015
Frequency of review:	Every 2 years

DOCUMENT AMENDMENT SHEET

Please record what changes you have made to the procedural document since the last version.

This is a detailed tracked change document and is designed to show people exactly what has changed. The version number recorded below should correspond to the ratified version number shown on the Document Summary Sheet.

Version	Amendment	Reason
0.1	N/A	First draft for consultation
0.2	Removal of references to Leeds Protocol. All hyperlinks updated TEWV logo added Final tidy and proof-read	Further review ahead of 1st ratification
1.0	Ratified	First version ratified

1. Introduction

This agreement is written to promote the sharing of personal data and / or sensitive personal data, as defined by the Data Protection Act (1998). It describes the information that will be shared between the partner organisations and arrangements for assisting compliance with relevant legislation and guidance, including the Data Protection Act (1998).

Information sharing agreements do not in themselves make the sharing of personal data and / or sensitive personal data legal or ethical. The Data Protection Act (1998) sets out the context in which information may be used legally, with this agreement echoing the legislative framework and promoting best practice and co-operation across partner organisations.

The following statement should guide all information sharing within the Information Sharing Partnership:

Whenever there is a need to share personal data and / or sensitive personal data, the specific reasons for sharing the information should be recorded, along with why it is considered relevant. The volume and detail of information shared must always be sufficient but not excessive for the required purpose. Wherever possible, decisions to share information should be made within the context of appropriate support, rather than by staff acting alone.

Where information is fully anonymised, or is otherwise non-identifiable or statistical in nature it is not necessary to apply this agreement. Care must be taken however to establish that information is fully anonymised, as the obvious fields of person-identifiable data may not be the only positive identifiers within shared material.

2. Background & Purpose

Leeds and York Partnership NHS Foundation Trust and TEWV have agreed to share personal data and / or sensitive personal data for the purposes listed below.

To provide direct clinical care to patients with an eating disorder To provide direct clinical care to patients of the forensic psychiatry service

The background to this is that in 2010 the North Yorkshire PCT was dissolved and its mental health and learning disability services acquired by TEWV and LYPFT. The latter acquired the Eating Disorders and Forensic Psychiatry Services for the TEWV locality, which has meant that since then, teams that previously worked for the same organisation and shared information as needed have since been divided by organisational boundaries. Information continues to be shared between the

clinicians, but LYPFT staff do not have access to the electronic patient records held by TEWV.

3. Information to be Shared

There are two distinct classifications of data covered by the Data Protection Act (1998): Personal data and sensitive personal data.

Personal data includes data relating to a living individual who can be positively identified from the data, or from the data and other information which is at the disposal of other individuals or is in the public domain. Personal data includes obvious identifiers such as names, addresses, dates of birth, as well as NHS or National Insurance numbers. Facial photographs and CCTV footage are also regarded as personal data, as are descriptions or photographic records of unique scars, tattoos or other markings.

Sensitive personal data includes data relating to racial or ethnic origins, religious beliefs or similar belief systems, political opinions and affiliations, trade union membership, physical or mental health (including disabilities), sexual life, the commission or alleged commission of offences, and criminal proceedings.

In respect of this agreement, the following types of information will be shared:

The complete care records for TEWV patients who have either an eating disorder clinician or forensic psychiatry practitioner from LYPFT working with them.

In practice, this will mean that LYPFT staff will need to access and make entries in the Community Mental Health (CMH) electronic care record (TEWV PARIS) where the Care Coordination takes place and where the complete care record resides.

Any information that links a service user to the receipt of mental health services is sensitive personal data. The data this agreement applies to, therefore, is sensitive, even at the index level.

4. Methods Used for Sharing Information

Information may be shared in the following ways:

- Information accessed in situ, via provision of access to organisational systems, databases, or records.
- In written information transferred by secure e-mail.
- In written communications transferred by fax.
- Documents transferred on CD, DVD or other electronic digital media.
- In written communications, (for example, alert / referral forms, letters, statements or reports) transferred in hard copy through internal or external mail or courier services.

- Verbally i.e. face to face, in wider meetings or on the telephone.

When any of these methods are used it is essential to consider the security of the access, processing and recording of information, and to ensure safe transit and delivery. Information should be appropriately secured in transit, transferred by methods aligned to the best practice specified in the Data Handling Procedures in Government: Final Report – June 2008.

Verbal conversations and interviews should be recorded in a statement that is agreed by the information giver. Care must be taken to record and denote information clearly as fact, statement or opinion and to attribute any statement or opinion to the owner. All information should be recorded in such a way that it can be used as evidence in court, should that be required at a later date.

Meetings should be recorded in minutes that are agreed by the delegates present.

Written communications containing confidential information should be transferred in a sealed envelope and addressed by name to the designated person within each organisation. They should be clearly marked "Private & Confidential".

When files are transferred on CD, DVD or other electronic digital media, the files should be encrypted to an appropriate standard, with decryption keys / passwords delivered separately.

When confidential information is sent by e-mail, it should be sent and received using secure government domain e-mail addresses, to ensure encryption of information in transit. Secure e-mails include the following e-mail address domains:

- Secure NHS email domain:
  - *.nhs.net
- Secure email domains in Central Government:
  - *.gsi.gov.uk
  - *.gse.gov.uk
  - *.gsx.gov.uk
- The Police National Network/Criminal Justice Services secure email domains:
  - *.police.uk
  - *.pnn.police.uk
  - *.scn.gov.uk
  - *.cjsm.net
- Secure email domains in Local Government/Social Services:
  - *.gcsx.gov.uk

In-transit security is reliant on BOTH the sender AND recipient using one of the e-mail domains listed above. In the absence of this, the SENDER will need to encrypt the content of the e-mail using additional software. This may be achieved by sending an encrypted attachment. Encryption software may be purchased or obtained from public domain sources for this purpose (e.g. WinZip, TrueCrypt etc), whilst document-level encryption is supported in business application suites such as Microsoft Office.

When confidential information is sent by fax, it should be sent to a 'safe haven' fax. This is a fax machine that is managed in such a way that the sender can be confident that information can be transferred to it in the knowledge that safeguards are in place to ensure its security and that access is restricted to assure confidentiality.

In all transfer scenarios, the onus is on the SENDER to ensure that:

- Information is transferred securely
- The chosen method is acceptable to and workable by the recipient
- Information has reached the required recipient

In the event that a recipient receives information by an unsecured route, it is incumbent on the recipient to advise the sender and agree a secure route for future transfers of information.

In respect of this agreement, information will be shared using the following methods:

The eating disorder and forensic services clinicians will be provided with access to the TEWV PARIS care record and will make all of their clinical entries into that record. No separate entries will be made into the LYPFT electronic record unless an in-patient episode occurs in LYPFT services.

5. The Need to Know

A prime consideration of access to or sharing of information is the 'Need To Know'.

Although access to information may be possible within the remit of a role, or access granted to systems on which information is stored, this does not necessarily mean that any individual should access information stored therein, or that they should access information beyond that which is necessary to perform a given task. This is best expressed as follows:

- Access to information should be on a strictly 'Need to Know Basis'.

- Records must only be accessed when there is a clear "legitimate relationship" between those accessing the records and the subject of the records.
- Within a legitimate relationship, the level of records access should be limited to that information which is relevant to task.

The patient is seen within the usual TEWV CPA policies and procedures and as such the complete care record is held by TEWV on its electronic care record (TEWV PARIS). The Eating Disorder and Forensic Services clinicians are co-workers for the time that they are working with the patient and as such become part of the clinical team with a full 'need to know' in order to provide direct patient care.

6. Consent from Individuals to Share their Personal Information

Staff and volunteers should always seek consent from individuals before sharing their personal data and / or sensitive personal data, whenever possible and appropriate. They should record the consent, when given, on their organisation's standard consent documentation, or as a contemporaneous entry into the electronic records system.

Where it is not possible to obtain consent, this could be because:

- the individual does not have the mental capacity to consent
- it may not be safe to seek consent
- it may not be possible to seek consent for some other reason

In cases where it has not been possible to seek or obtain consent, staff or volunteers should always record the justification for sharing the information, and how this decision was arrived at.

1. If the individual does not have the mental capacity to consent, staff or volunteers should record this using their agency's Mental Capacity Assessment recording tool or other appropriate method, and record their decisions to share information using their agency's Best Interests Decision recording tool or other appropriate method.

2. If the subject has not given consent for reasons other than those covered by the Mental Capacity Act, one of the reasons from Schedule 2 of the Data Protection Act (1998) is required to justify the sharing of personal data, whilst a reason from Schedule 2 AND Schedule 3 is required to share sensitive personal data. Those reasons with particular relevance to this agreement are included below:

Schedule 2 – Justifications for the sharing of personal data:

- Compliance with the legal obligations of partner organisations

- Protecting the vital interests of the subject
- Carrying out tasks or duties substantially in the wider public interest
- **Pursuing the legitimate interests of the partner organisation**

Schedule 3 – Justifications for the sharing of sensitive personal data:

- Compliance with employment law obligations
- Protecting the vital interests of the subject
- Legal advice and establishing or defending legal rights
- Public functions (including the administration of justice)
- **Medical purposes and the provision of healthcare**
- Detection of unlawful activity
- Protection of the public
- Confidential counselling
- Police processing

For further advice on justifiable grounds for sharing information, contact your organisation's Data Protection specialist or Caldicott Guardian. If your organisation does not have such a role, your line manager may be able to advise you on the most appropriate source of guidance.

7. Information Retention and Disposal

The Data Protection Act (1998) requires that personal data and sensitive personal data are not retained for longer than necessary. Partner organisations may have their own organisational, legal or procedural requirements for records retention and disposal. These retention schedules should be observed and applied at all times.

Where no such organisational procedure exists, it is essential to keep pertinent information as long as there continues to be a need, and equally that such information is securely disposed of when no longer required.

LYPFT and TEWV administer their retention and disposal processes in line with the NHS Code of Practice for Records Management. Retention and disposal will therefore be dictated by classifying the data against the NHS Code and enacting the required retention and disposal regime. Where there are local differences to the clinical record the TEWV retention schedule will take priority.

8. Dissemination & Training

Each partner organisation should develop their own approach to dissemination of this agreement and the provision of awareness and training to support its use.

9. Access Agreements

Where information is to be shared via granting inter-organisational access to systems operated by partner organisations, the 'owning' organisation of the system will draft and agree an Access Agreement with the partner organisation to govern the activities of partner staff using the system.

A template for this purpose is available on request.

Where access to systems is to be granted, staff will be required to complete any training stipulated by the system owning organisation as a pre-requisite of access.

10. Discipline

Although this agreement seeks to promote the sharing of information between partner organisations, use of the information shared should never exceed the purposes or intentions of the original reason for sharing.

Where allegations are made that information has been used inappropriately, or that the confidentiality of subjects has been breached, partner organisations will co-operate in a full and frank investigation of these allegations.

In the event that any wilful misconduct is substantiated which resulted in a breach of subject confidentiality, this will be regarded as an act of serious or gross misconduct and actioned accordingly.

Instances of inappropriate access to electronic records may be regarded as criminal action under both Section 55 of the Data Protection Act (1998) and Section 1 of the Computer Misuse Act (1990), and may result in a custodial sentence. (r vs Dale Trever, 2010).

Sharing partners should maintain an awareness of current relevant legislation.

With effect from 1st June 2013, Health and Social Care organisations are obliged to grade and report information governance / data protection breaches against the new SIRI grading and reporting regime. Incidents which are rated as severity 2 or higher will be reported via the online tool and automatically escalate for scrutiny to the ICO, DoH, CQC and other regulators.

11. Performance of this Agreement

Should any member of staff or volunteer working for a partner organisation feel that the letter and spirit of this agreement is not being honoured, or that barriers to legitimate sharing of information are being raised, this should be communicated to

their organisation's Information Sharing or Information Governance lead, who will in turn follow this up with their counterparts in the partnership organisation(s).

12. Supporting Documentation

ICO Data Sharing Code of Practice

Data Handling Procedures in Government: Final Report – June 2008

NHS Confidentiality Code of Practice – November 2003

Caldicott review: information governance in the health and care system – April 2013

13. Signatories to the Agreement

Approved by : Dr Jim Isherwood – Caldicott Guardian

signed

For : Leeds and York Partnership NHS Foundation Trust

Date : 03/10/2013

Approved by : Chris Stanbury- Caldicott Guardian

Signed

For : Tees, Esk and Wear Valleys NHS Foundation Trust

Date : 30/09/2013

A copy should be sent to the Data Protection Officer / Caldicott Guardian of each partner organisation for approval and signature. In the absence of the above roles an appropriate senior signatory will suffice.

Copies of this Agreement should be retained by the named persons above and be made available for inspection.