The Leeds Teaching Hospitals NHS
NHS Trust

Dated 14/07/2011

Information Sharing Agreement

between

The Leeds Teaching Hospitals NHS Trust

and

Leeds Partnerships NHS Foundation Trust

Access to E-Results Service

Document Control

Revision History		
Issue	**Date**	**Revision Details**
1	**22/06/2011**	
2	**11/07/2011**	Amended to reflect changes requested by Carl Starbuck, Information & Knowledge Manager, Leeds Partnerships NHS Foundation Trust.
3	**14/07/2011**	Amended to reflect changes requested by Carl Starbuck, Information & Knowledge Manager, Leeds Partnerships NHS Foundation Trust.

1. Introduction

The management of information by partner organisations is often necessary to ensure the highest quality of care from integrated services.

To ensure that patients and their representatives receive the highest standards of care, support and protection, it is essential that partner organisations (or 'agencies') work together effectively and efficiently. The successful management of information is fundamental to ensure co-ordinated and 'seamless' care for the patient.

This Information Sharing Agreement (the **Agreement**) is to support information sharing for services that will be provided into the future to meet the needs and changing demands of the local health community. This Agreement has been drawn up with reference to the framework of the Leeds Interagency Protocol for Sharing Information (the **Protocol)**. Further information on the Protocol can be found in Appendix C.

1.1. Parties to the Agreement

This Agreement is between Leeds Partnerships NHS Foundation Trust (**LPFT**), and the Leeds Teaching Hospitals NHS Trust (**LTHT**). It is acknowledged that the host of the e-Results system is the Data Processor in respect of this agreement, and that organisations treating the patient and requesting tests/results is the Data Controller.

1.2. Scope of the Agreement

This document outlines the controls and measures for the use of data for the provision of services and treatment of patients.

This Agreement covers access to the LTHT E-Results Service by all employees, agency workers and volunteers of the above party organisations.

1.3. Defined Purpose of the Agreement

The defined purpose (the **Purpose**) of this Agreement is as follows:

LPFT require remote access to LTHT's E-Results Service in order to reduce or mitigate risks associated with the receipt of service user test results. User access to the E-Results Service is limited to those users specifically verified by LPFT's Information Governance team and authorised by LTHT.

Detailed information on the Purpose can be found in Appendix B and C.

1.4. Objectives of the Agreement

The objectives of the Agreement are:

- To provide a framework for the secure and confidential management of information for Health Organisations.

- To confirm the principles and procedure agreed by partner organisations concerned with the obtaining, holding and sharing of information about individuals.

- To recognise that each partner organisation will have their own local policies and procedures regarding information security and confidentiality and to make clear that this Agreement is not designed to supersede existing local policies but to compliment and support such policies.

- To define the specific purpose for use of the shared information.

- To define the responsibilities of partners to the Agreement to implement internal arrangements to meet its requirements.

- To define how the Agreement will be implemented, monitored and reviewed.

2. Agreement Requirements

2.1. Operational Requirements

All parties to the Agreement will manage information 'in confidence', with all staff having awareness of the 'common law' duty of confidentiality and data protection and their obligation to safeguard the confidentiality of personal information. Parties to the Agreement should underpin this duty with references to it in contracts of employment and/or codes of conduct. This will be achieved by:

- Ensuring that local mechanisms exist so that personal information is kept secure and confidential.

- Ensuring that all personal information that is shared under this Agreement meets any statutory requirement, particularly the processing conditions for compliance with the Data Protection Act 1998, including:

    - Arrangements for informing patients of the sharing of information and or services.
    - Staff training to assist consent seeking and data protection understanding.
    - Dealing with circumstances when the service user is unable to give consent.
    - Practical arrangements to record consent granted or withheld for easy future reference.
    - To ensure there are policies and procedures to support secure data sharing and that they are implemented, monitored and kept up-to-date.

- Ensuring that where information is disclosed outside the scope of the Agreement without or against the consent of the individual because the information is required by a court order/statute or there is an overriding public interest in doing so, the decision to release information should be made according to the Data Protection Act 1998, Confidentiality: NHS Code of Practice, and Joint Working

Authority Agreement. The judgement must be made on a case-by-case basis. It may be appropriate to seek additional legal or specialist advice if information is to be disclosed without the individuals' consent and breaches the duty of confidentiality previously owed. A record should be kept as to the reason why a disclosure of personal information was made. Where public interest is the reason, the grounds for doing so should be documented.

- Ensuring if an individual wants information about them withheld from a third party (who might otherwise have received it) then the individuals' wishes are respected unless there are exceptional circumstances. Every effort should be made to explain to the individual the consequences for care and planning, but the final decision should rest with the individual.

- Ensuring that adequate provision exists locally to address complaints relating to any disclosures of information.

- Ensuring partners to the agreement immediately inform the other of any breaches to the security of the LTHT E-Results Service or of the terms of this Agreement.

- Ensuring that local mechanisms exist to address data quality issues, including:

    - The identification of local staff with responsibility for the quality of shared data ensuring that partner organisation data is not updated inaccurately or inappropriately deleted.
    - Retraining of staff as required.

- Ensure that partner organisations have mechanisms in place for the appropriate disclosure of information to the public under the terms of the Data Protection Act and Freedom of Information Act. Requests for information should be dealt with by the organisation treating the patient, but should ensure that only data for which they are data controller is disclosed.

- Ensure that there is an annual data protection review and that there is a valid and up-to-date registration with the Information Commissioner.

2.2. Security Requirements

Each partner organisation will ensure that adequate security policies and procedures are in place and are implemented, adhered to and monitored for compliance. These policies (where appropriate) will be available to partner organisations; however some policies may remain undisclosed in order to ensure the protection of local infrastructures.

Where the infrastructure is shared trust policies should be standardised.

The host authority will implement security and confidentiality procedures including backup and continuity plans that will ensure compliance.

Each partner organisation will be responsible for the quality and security of data that is processed by their staff.

Information management at an operational level will be the subject of respective Individual Policies, Procedures and Guidelines, as required.

Staff will only have access to personal information on a 'need to know' basis in order to perform their duties in connection with the Purpose. Should an information breach occur, partner organisations will take action according to their local disciplinary policies.

The partners to the Agreement will take all reasonable care and safeguards to protect both the physical security of information technology and the data contained within it. They will ensure that mechanisms are in place to address the issues of physical security, security awareness and training, transporting of confidential information procedures, security management, systems development and system specific security policies. Organisations must have an Information Security Policy.

3. Procedures to manage the Agreement

3.1. Formal Approval and Adoption

Formal adoption will follow the signing of the document by the Caldicott Guardian (or equivalent) and Head of Information Governance or Senior lead of each partner organisation. Amendments, additions or deletions may be made to the Agreement if ratified by each proposed partner organisation prior to signature.

3.2. Availability

The Agreement will be freely available to any representative of any organisation that manages patient identifiable information with a view to the Purpose.

Local arrangements will exist to ensure the Agreement is available for public scrutiny to supplement information already provided to the general public on matters of information sharing under the Freedom of Information Act 2000.

3.3. Monitor and Review

The service will commence from June 2011 and is ongoing. The Agreement will be reviewed annually from the date of signing. In addition, the Agreement will be subject to formal review following pertinent changes to law, ethics and policy in relation to the security and confidentiality of information.

The use and effectiveness of the Agreement will be evaluated as follows:

- Non-compliance with the Agreement may be logged and reported by any partner organisation, including complaints arising as a result of information sharing.

- Non-compliance to any supplemental policies, procedures and guidelines may be logged and reported by any partner organisation, including complaints arising as a result of information sharing.
- Any general difficulties encountered in applying the Agreement may be logged and reported by any partner organisation.

4. Formal approval of the Agreement

The parties to the Agreement accept that the procedures within it will provide a secure framework for information sharing in a manner compliant with their statutory and professional responsibilities. Where appropriate this Agreement will be supplemented by Individual Policies, Procedures and Guidelines, further defining the information management arrangements between partner organisations.

On behalf of The Leeds Teaching Hospitals NHS Trust (LTHT), the following authorised signatories agree to the terms set out in this Agreement.

Name: Balbir Bhogal

Designation: Deputy Director of Informatics - Information and Patient Services

Signature: …**Balbir Bhogal**…… Date: …**05/08/2011**……..

On behalf of Leeds Partnerships NHS Foundation Trust (LPFT), the following authorised signatory agrees to the terms set out in this Agreement.

Name: Douglas Fraser

Designation: Caldicott Guardian

Signature: …**Dr Douglas Fraser**…… Date: …**16/08/2011**……..

Appendix A

Name of Partner Organisation(s):

The Leeds Teaching Hospitals NHS Trust
St James Hospital
Beckett Street
Leeds
LS9 7TF
0113 20433144

Leeds Partnerships NHS Foundation Trust
2150 Thorpe Park
Century Way
Colton
Leeds
LS15 8ZB
0113 305 5952

Appendix B

Additional background information:
LPFT require remote access to LTHT's E-Results Service in order to reduce or mitigate risks associated with the receipt of service user test results. User access by LPFT staff to the LTHT E-Results Service is limited to those users specifically verified by LPFT's Information Governance team and authorised by LTHT.

LTHT's Information Governance Group has mandated that access to the E-Results Service be in accordance to the Data Protection Act 1998, Caldicott Principles and LTHT policy. Any detected breaches in the guidelines detailed within the E-Results Service User Access Policy provided by LTHT to LPFT will be subject to investigation and must be reported to the LTHT Information Governance and Data Protection Manager. All reported breaches may invoke the local organisation Disciplinary Procedure which may result in formal or final warnings, employment suspension or termination. Proven instances of inappropriate access to records may result in the involvement of West Yorkshire Police and investigation/prosecution under the Computer Misuse Act 1990.

All staff approved to access LTHT patient information via the E-Results Service must be trained in Information Governance and PC skills/literacy. Users who have not been suitably trained will have their access rights revoked until their training is brought up to date.

List of access rights:

- Individuals will have role-based access that has been assessed and approved on a 'need to know' basis.
- Individuals will only be granted access after having completed appropriate training.
- Access will be monitored and updated regularly.

Appendix C

Legislation and Guidance:

- The Adoption Act 1976
- The Mental Health Act 1983
- The Copyright, Designs and Patents Act 1988
- The Access to Health Records Act 1990
- The Computer Misuse Act 1990
- The NHS and Community Care Act 1990
- The Carers Act 1995
- The Data Protection Act 1998
- The Crime & Disorder Act 1998
- The Human Rights Act 1998
- The Health Act 1999
- The Freedom of Information Act 2000
- The Health & Social Care Act 2001
- Common Law Duty of Confidence

Other Guidance:

- Caldicott Committee Report
- British Standard ISO 17799 (BS 7799)
- Policies, Procedures and Guidelines

The Protocol:

The Protocol is an over-arching framework for sharing information between health, social care and other agencies in Leeds. It focuses on requirements for sharing personal information about service users. The Protocol:

- Clarifies the legal background on information sharing.
- Outlines the principles that need to underpin the process.
- Provides practical guidance on how to share information in a series of supporting Procedures.
- Provides a framework within which organisations can develop Information Sharing Agreements (ISAs) or Access Agreements for specific areas of service.
- Includes arrangements for monitoring and reviewing the use of the Protocol and for responding to breaches.

Both LTHT and LPFT are parties to the Protocol. The Protocol is not contractually binding but is to be used to set good practice standards that the parties need to meet in order to fulfil any duty of care which exists in relation to the sharing of personal information.

The procedures referenced under this Agreement are detailed in the document titled '**Operational Procedures Governing the Sharing of Information between Agencies in Leeds'.**