Lincolnshire Inter-Agency Information Sharing Protocol

Document Control

Reference	Lincolnshire Inter-Agency Information Sharing Protocol
Date	1 May 2017
Version	6.5

Version History

Date	Version Number	Revision Notes	Status
27 January 2015	V 6	This document replaces the "Lincolnshire Overarching Information Sharing Protocol" V 5.4. It incorporates a new document structure and content refresh across its entirety.	Out for consultation.
20 March 2015	V6.1	Amendments following feedback from Countywide IG Group: Para 3 – Reference to MoPI and ICO guidance added. Para 4.2 – Reference to Schedules 2 and 3 of the Data Protection Act added. Para 5.4 – Amended, includes implementing local controls to identify patterns of ad hoc sharing. Para 6 – Added para referencing situations where minimum security standards cannot be achieved. Para 6.1 – Minor amendment to text. Para 6.3 – "GCSX" removed and replaced with "formally accredited". Para 7 – Individual rights added.	Submitted for final review.
11 May 2015	V6.2	Signatories agreed and added.	Published
13 May 2015	V6.3	Lincolnshire Partnership Foundation Trust added to signatory list.	Published
1 May 2017	V6.4	Protocol reviewed and updated.	Published
30 May 2017	V6.5	CCGs were added to the document.	Published

Contents

Partner Organsations

The following organisations are signatories to the Lincolnshire Inter-Agency Information Sharing Protocol:

- East Midlands Ambulance Trust
- Lincolnshire Community Health Services NHS Trust
- Lincolnshire County Council
- Lincolnshire Partnership NHS Foundation Trust
- Lincolnshire Police
- NHS Lincolnshire East Clinical Commissioning Group
- NHS South Lincolnshire Clinical Commissioning Group
- NHS South West Lincolnshire Clinical Commissioning Group
- NHS Lincolnshire West Clinical Commissioning Group
- North West Anglia NHS Foundation Trust
- St Barnabas Hospice
- United Lincolnshire Hospitals NHS Trust

Signatory:

Each organisation is required to agree and support this agreement by signing their individual signature sheet (Appendix A).

1. Introduction

Effective sharing of information across organisational and professional boundaries plays a crucial role in providing efficient services to the public across a range of sectors. It is important to maintain trust in the way information is shared by demonstrating that it is done so in a lawful, responsible and secure manner.

Whilst it is recognised and acknowledged that each participating organisation will have their own specific organisational information governance requirements, it is necessary to adopt a partner neutral approach based on key objectives equally important and necessary to all instances of information sharing.

This strategic protocol aims to support this approach by identifying and agreeing key objectives designed to facilitate appropriate and lawful sharing of information between partner organisations in Lincolnshire.

The protocol is not designed to replace the need for individual information sharing agreements nor is it designed to articulate in detail legislative or partner specific requirements.

2. Scope

This protocol is applicable to all instances of information sharing involving personal data and sensitive personal data[1] between partner organisations and is agreed by Senior Information Risk Owners, or equivalent, of participating organisations.

3. Key Objectives

Partner organisations agree the following key objectives:

- To endorse, support and promote the accurate, timely, and secure sharing of appropriate personal data;

- To maintain public confidence in public services by ensuring that information is shared lawfully and fairly within the framework of legal, statutory and common law requirements e.g. the Data Protection Act 1998, the Human Rights Act 1998 (article 8), the Common Law Duty of Confidence; and the General Data Protection Regulation (GDPR, as of May 2018).

- To consider specific sector legislation relevant to individual instances of information sharing e.g. the Children Act 1989 & 2004; the Health and Social Care Act 2012; the Crime and Disorder Act 1998.

- To ensure the Caldicott Principles and Health and Social Care Code of Practice on Confidential Information are considered when sharing health and social care information;

- To ensure the Management of Police Information (MoPI) guidance is considered when sharing police information.

---

[1] Personal data and sensitive personal data as defined by the Data Protection Act 1998

- To ensure appropriate guidance from the Information Commissioner's Office is considered e.g. Data Sharing Code of Practice

- To implement and apply organisational policies and procedures which facilitate information sharing and to ensure staff are aware of their information responsibilities;

- To promote and maintain a consistent and transparent approach to information sharing;

- To reduce organisational and individual risk caused by inappropriate or insecure sharing of information;

- To support instances of systematic information sharing through documented and agreed information sharing agreements, or equivalent.

4. Deciding to Share Personal Data

4.1. Factors to consider before sharing

Before sharing personal data partner organisations will carefully consider the following factors:

- What is the sharing meant to achieve?
- What is the legal basis for sharing the information?
- What information needs to be shared?
- Who requires access to the shared personal data?
- When and how should it be shared?
- How can we check the sharing is achieving its objectives?
- What risk does the data sharing pose?
- Could the objective be achieved without sharing the data or by anonymising it?
- How will any shared data be kept up to date?

4.2. Conditions for Sharing

Partner organisations shall share personal data fairly and lawfully and only when one or more conditions under the first data protection principle are satisfied.

Sharing involving sensitive personal data will be undertaken only when a further more exacting condition has been satisfied in accordance with the first data protection principle.

Conditions for processing are set out in Schedules 2 and 3 of the Data Protection Act.

Partner organisations acknowledge that meeting a condition for processing will not in itself ensure that the sharing of personal data is fair or lawful; these issues will be considered separately.

5. Fairness and transparency

Partner organisations will ensure that personal data is shared fairly and in a way that is reasonable. This means that people should generally be aware of which organisations are sharing their personal data and what it is being used for.

5.1. Privacy Notices

Partner organisations will maintain and review appropriate privacy notices in line with the Information Commissioners Office Code of Practice. Privacy notices will explain who the organisation is; why information is being shared and who it is being shared with.

Where necessary a privacy notice will be actively communicated.

5.2. Telling Individuals about Information Sharing

Whilst the primary responsibility for telling individuals about information sharing falls to the organisation that collected the data initially, partner organisations will work together to ensure that the individuals concerned know who has, or will have, their data and what it is being used for, or will be used for.

5.3. Sharing without the individual's knowledge

In certain limited circumstances the Data Protection Act 1998 provides for personal data, even sensitive data, to be shared without the individual knowing about it, for example:

- In the prevention or detection of crime;
- In the apprehension or prosecution of offenders; or
- In the assessment or collection of tax or duty.

Where it is known that the purpose for sharing the information does not require consent, the legal basis for not obtaining consent will be detailed within the specific information sharing agreement.

5.4. Ad hoc or 'one off' sharing

It may not always be possible to document the sharing of information in an emergency or time dependent situation and sharing may depend primarily on the exercise of professional judgement. Where this is the case partner organisations will make a record as soon as possible, detailing the circumstances, what information was shared and explaining why the disclosure took place.

In the event that ad hoc instances of information sharing become a regular occurrence, it will be considered whether it is necessary to amend an existing information sharing agreement to reflect this change or whether a separate information sharing agreement is required. Partner's organisations will consider implementing local controls to identify such patterns of ad hoc behaviour

6. Security of Personal Data

Although partner organisations might not remain liable for personal data shared with another partner it is incumbent on them to ensure that the data will continue to be protected with adequate security controls.

It is acknowledged that partners will have varying degrees of technical, physical and procedural security controls in place, some of which are driven by external compliance requirements e.g. PSN, CJX, NHS IG Toolkit. It is important therefore to ensure consistency in approach by agreeing common minimum standards which can be achieved by all partners and which provides appropriate assurance when sharing personal data.

Where minimum standards cannot be achieved e.g. because of conflict with local policy or an inability to apply technical controls to legacy systems processing electronic information, this will be acknowledged and documented within the relevant sharing agreement and a risk managed approach is to be agreed.

Notwithstanding specific security controls communicated and formalised by all parties within the relevant information sharing agreement, (the type and complexity of which will vary) partners agree the following minimum standards.

6.1. Minimum Security Standards

All staff involved in handling personal data shall complete locally arranged information security/data protection training commensurate with their role and in line with their own organisational requirements.

A security policy must be in place which sets out management commitment to information security and data protection and defines information security and data protection responsibilities.

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

6.2. Electronic Information

In accordance with each organisation’s policy electronic copies of personal data supplied shall only be stored:

- On hardware located in premises which are physically secure.
- On portable devices e.g. laptops, netbooks, which are encrypted using AES 256 bit encryption.
- Portable devices e.g laptops are to be transported in the boot of a car.
- On removable media e.g. USB memory sticks, CD's, DVD's and external hard drives which are encrypted using AES-256 bit encryption

Electronic personal data shall not be transferred to privately owned ICT e.g. a private laptop belonging to a staff member.

Portable devices and removable media shall be held under lock and key when not in use.

Passwords shall be a minimum of eight characters and should include a combination of upper and lower case letters, numbers and the special keyboard characters.

Electronic copies of personal data shall be securely deleted when no longer required (in line with local retention and disposal schedules). This includes data stored on servers, desktops, laptops or other hardware and media. Secure deletion means deleting files so they cannot be retrieved.

6.3. Electronic Data Transfer

Data transfer shall be achieved in a secure manner such as secure email (accredited to ISO27001); by secure file transfer; via a trusted private network (utilised for the exchange of information without data traversing the public internet); or by secure courier services.

Formally accredited secure email e.g. GCSX, NHS.Net, PNN, GSI, GSX shall be used where appropriate.

Where formally accredited secure email transfer is unavailable then an alternative secure email service shall be used. A secure email service is one which uses an encrypted communication/connection to deliver the email.

Where data transfer can only be achieved via removable media it shall be achieved using a signature service provided by a reputable secure courier and the removable media shall be encrypted using AES 256 encryption. Passwords must be communicated separately and will not be included with the media. The receiving party must confirm by email that they are ready for the transfer and that the recipient address is correct before the transfer takes place. A further email must be sent confirming when the recipient has received, intact, the data.

6.4. Network Security

Personal data stored on a device/network which connects to the public internet shall implement the following controls which offer a sound foundation of basic security:

- Boundary firewall and internet gateways.
- Secure configuration.
- User access control.
- Malware protection.
- Patch Management.

6.5. Hard Copy Information

Hard copy personal data which includes printed material, files, and documents shall be stored under lock and key when not in use and access to the information shall be controlled.

When printing off personal data only print the minimum necessary to achieve your aim.

When transporting hard copy personal data ensure it is done so securely e.g. a locked briefcase or bag.

Personal data shall only be removed from premises when absolutely necessary and shall be returned and locked away as soon as possible.

Hard copy personal data shall be destroyed securely when no longer required e.g. cross cut shredder. Alternatively it can be returned securely to the originating partner for destruction if local facilities are not available.

Data transfer of hard copy personal data shall be achieved by signature service recorded delivery or courier service in a sealed envelope, addressed to an individual by name or appointment.

6.6. Security Incidents/Data Breaches

The receiving partner organisation shall notify the originating partner organisation immediately of any information which has been subject to an actual or potential security incident or data breach including any failure to comply with the security requirements set out in the information sharing agreement.

In the event of a security incident or data breach data transfers may be delayed until the risk or issue is resolved.

If a security incident or data breach cannot be resolved following intervention data transfers shall stop unless the risk of stopping the transfer of personal data is outweighed by the need to transfer the personal data. Authority to continue must be provided by the originating Data Controller.

7. Individual Rights

The Data Protection Act gives individuals certain rights over their personal data.

These include:

• the right to access personal data held about them;

• the right to know how their data is being used; and

• the right to object to the way their data is being used.

Partner organisations will provide clear information for individuals about how they can access their data and make this process as straightforward as possible

In addition partner organisations will have systems in place to allow prompt location and access to personal data in response to requests and will ensure a response is provided within the statutory requirements set out by the Data Protection Act 1998. .

Individuals can object where the use of their personal data is causing them substantial, unwarranted damage or substantial, unwarranted distress however the Act does not provide the individual with an unqualified right to stop their personal data being shared.

Partner organisations will have processes in place to respond to objections which reflect the requirements of the Data Protection Act 1998.

If a significant number of objections, negative comments or other expressions of concern are received, a review of the data sharing in question will be carried out.

8. Governance

Partner organisations will ensure appropriate governance is in place to take on overall responsibility for information governance, ensuring compliance with the law, and providing advice to staff.

9. Information Sharing Agreements

Partner organisations will aim to document instances of systematic information sharing within documented information sharing agreements (ISA). The ISA's shall include:

- The purpose, or purposes, of the sharing;
- The potential recipients or types of recipient and the circumstances in which they will have access;
- The data to be shared;
- The process for sharing;
- Data quality – accuracy, relevance, usability etc;
- Data security;
- Retention of shared data;
- Individuals' rights – procedures for dealing with access requests, queries and complaints;
- Review of effectiveness/termination of the sharing agreement; and
- Sanctions for failure to comply with the agreement or breaches by individual staff.

10. Review of the Lincolnshire Inter-Agency Information Sharing Protocol

As a minimum this protocol will be reviewed on annual basis from the date of issue by the Countywide Information Governance Management Group.

Appendix A

Signatory: East Midlands Ambulance Trust

I (the Caldicott Guardian / SIRO) agree to support and implement the Lincolnshire Inter-Agency Information Sharing Protocol in order to facilitate appropriate and lawful sharing of information between the specified partner organisations.

Name:	
Role:	
Signature:	
Date:	

Each organisation is required to keep a copy of their signed agreement and send a copy to the Chair of the* Countywide Information Governance Management Group *in order to them to be collated and attached to the original protocol.

Signatory: Lincolnshire Community Health Services NHS Trust

I (the Caldicott Guardian / SIRO) agree to support and implement the Lincolnshire Inter-Agency Information Sharing Protocol in order to facilitate appropriate and lawful sharing of information between the specified partner organisations.

Name:	
Role:	
Signature:	
Date:	

Each organisation is required to keep a copy of their signed agreement and send a copy to the Chair of the* Countywide Information Governance Management Group *in order to them to be collated and attached to the original protocol.

Signatory: Lincolnshire County Council

I (the Caldicott Guardian / SIRO) agree to support and implement the Lincolnshire Inter-Agency Information Sharing Protocol in order to facilitate appropriate and lawful sharing of information between the specified partner organisations.

Name:	
Role:	
Signature:	
Date:	

Each organisation is required to keep a copy of their signed agreement and send a copy to the Chair of the* Countywide Information Governance Management Group *in order to them to be collated and attached to the original protocol.

Signatory: **Lincolnshire Partnership NHS Foundation Trust**

I (the Caldicott Guardian / SIRO) agree to support and implement the Lincolnshire Inter-Agency Information Sharing Protocol in order to facilitate appropriate and lawful sharing of information between the specified partner organisations.

Name:	
Role:	
Signature:	
Date:	

Each organisation is required to keep a copy of their signed agreement and send a copy to the Chair of the **Countywide Information Governance Management Group** ***in order to them to be collated and attached to the original protocol.***

Signatory: Lincolnshire Police

I (the Caldicott Guardian / SIRO) agree to support and implement the Lincolnshire Inter-Agency Information Sharing Protocol in order to facilitate appropriate and lawful sharing of information between the specified partner organisations.

Name:	
Role:	
Signature:	
Date:	

Each organisation is required to keep a copy of their signed agreement and send a copy to the Chair of the* Countywide Information Governance Management Group *in order to them to be collated and attached to the original protocol.

Signatory: **NHS Lincolnshire East Clinical Commissioning Group**

I (the Caldicott Guardian / SIRO) agree to support and implement the Lincolnshire Inter-Agency Information Sharing Protocol in order to facilitate appropriate and lawful sharing of information between the specified partner organisations.

Name:	
Role:	
Signature:	
Date:	

Each organisation is required to keep a copy of their signed agreement and send a copy to the Chair of the **Countywide Information Governance Management Group** ***in order to them to be collated and attached to the original protocol.***

Signatory: **NHS South Lincolnshire Clinical Commissioning Group**

I (the Caldicott Guardian / SIRO) agree to support and implement the Lincolnshire Inter-Agency Information Sharing Protocol in order to facilitate appropriate and lawful sharing of information between the specified partner organisations.

Name:	
Role:	
Signature:	
Date:	

Each organisation is required to keep a copy of their signed agreement and send a copy to the Chair of the **Countywide Information Governance Management Group** ***in order to them to be collated and attached to the original protocol.***

Signatory: **NHS South West Lincolnshire Clinical Commissioning Group**

I (the Caldicott Guardian / SIRO) agree to support and implement the Lincolnshire Inter-Agency Information Sharing Protocol in order to facilitate appropriate and lawful sharing of information between the specified partner organisations.

Name:	
Role:	
Signature:	
Date:	

Each organisation is required to keep a copy of their signed agreement and send a copy to the Chair of the **Countywide Information Governance Management Group** ***in order to them to be collated and attached to the original protocol.***

Signatory: **NHS Lincolnshire West Clinical Commissioning Group**

I (the Caldicott Guardian / SIRO) agree to support and implement the Lincolnshire Inter-Agency Information Sharing Protocol in order to facilitate appropriate and lawful sharing of information between the specified partner organisations.

Name:	
Role:	
Signature:	
Date:	

Each organisation is required to keep a copy of their signed agreement and send a copy to the Chair of the* Countywide Information Governance Management Group *in order to them to be collated and attached to the original protocol.

Signatory: North West Anglia NHS Foundation Trust

I (the Caldicott Guardian / SIRO) agree to support and implement the Lincolnshire Inter-Agency Information Sharing Protocol in order to facilitate appropriate and lawful sharing of information between the specified partner organisations.

Name:	
Role:	
Signature:	
Date:	

Each organisation is required to keep a copy of their signed agreement and send a copy to the Chair of the **Countywide Information Governance Management Group** ***in order to them to be collated and attached to the original protocol.***

Signatory: **St Barnabas Hospice**

I (the Caldicott Guardian / SIRO) agree to support and implement the Lincolnshire Inter-Agency Information Sharing Protocol in order to facilitate appropriate and lawful sharing of information between the specified partner organisations.

Name:	
Role:	
Signature:	
Date:	

Each organisation is required to keep a copy of their signed agreement and send a copy to the Chair of the **Countywide Information Governance Management Group** ***in order to them to be collated and attached to the original protocol.***

Signatory: United Lincolnshire Hospitals NHS Trust

I (the Caldicott Guardian / SIRO) agree to support and implement the Lincolnshire Inter-Agency Information Sharing Protocol in order to facilitate appropriate and lawful sharing of information between the specified partner organisations.

Name:	
Role:	
Signature:	
Date:	

Each organisation is required to keep a copy of their signed agreement and send a copy to the Chair of the* Countywide Information Governance Management Group *in order to them to be collated and attached to the original protocol.