Lincolnshire Inter-Agency Information Sharing Protocol

Document Control

Reference	Lincolnshire Inter-Agency Information Sharing Protocol
Date	
Version	7

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
Nov 2018	V 7	Full review.	Out for Consultation
28 Mar 2019	V7	Approved document and completed signatory list	Published

Contents

Partner Organsations

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

- East Midlands Ambulance Service NHS Trust
- Lincolnshire Community Health Services NHS Trust
- Lincolnshire County Council (inc District Councils)
- Lincolnshire East Clinical Commissioning Group
- Lincolnshire Partnership NHS Foundation Trust
- Lincolnshire Police
- Lincolnshire South Clinical Commissioning Group
- Lincolnshire South West Clinical Commissioning Group
- Lincolnshire West Clinical Commissioning Group
- 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 does not constitute an appropriate governance arrangement for any instance of systematic information sharing. This must be documented on a case by case basis taking account of the circumstances and legal framework surrounding that particular processing activity.

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 (SIRO), 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 (DPA) 2018 including the General Data Protection Regulation (GDPR), the Human Rights Act 1998 (article 8) and the Common Law Duty of Confidence.

- 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 (this act is not exhaustive).

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

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

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

[1] Personal data as defined by the General Data Protection Act Regulation

- 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 (ISA), 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 when a lawful basis for processing has been identified.

Partner organisations shall share personal data in a manner consistent with the data protection principles set out at Article 5 of the GDPR and Chapter 2 of Part 3 of the DPA 2018, where processing is for law enforcement purposes.

The sharing of personal data will only be considered lawful if it falls within one of the lawful bases defined within Article 6 of the GDPR. Sharing involving special category data is strictly prohibited unless it satisfies at least one of the additional lawful bases set out at Article 9 of the GDPR and/or Schedule 1 of the DPA 2018.

If personal data is processed for law enforcement purposes and the sharing constitutes 'sensitive processing'[2] then it must meet one of the conditions set out in Schedule 8 of the DPA 2018.

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.

[2] Defined by Section 35(8) of the DPA 2018

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 Notice / Fair Processing Notice

Partner organisations have a statutory duty to ensure that individuals are appropriately informed about the collection and use of their personal data. In order to meet this duty, partner organisations will each ensure that adequate privacy information is made available to service users.

https://www.emas.nhs.uk/your-service/your-information/

https://www.lincolnshirecommunityhealthservices.nhs.uk/about-us/information-governance/fair-processing-notice

https://www.lincolnshire.gov.uk/privacy-notices/privacy-notice-lincolnshire-county-council/132493.article

https://lincolnshireeastccg.nhs.uk/about-us/privacy-notice

http://www.lpft.nhs.uk/site/privacy-policy

https://www.lincs.police.uk/resource-library/data-protection/privacy-notice/

https://southlincolnshireccg.nhs.uk/about-us/privacy-notice

http://southwestlincolnshireccg.nhs.uk/privacy-notice

https://www.lincolnshirewestccg.nhs.uk/about-us/fair-processing-notice/

https://stbarnabashospice.co.uk/privacy-policy/

https://www.ulh.nhs.uk/fair-processing-notice/

5.2. Informing 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 DPA provides for both personal data and special category data to be shared without the individual knowing about it. Schedules 2, 3 and 4 of the DPA 2018 set out the specific circumstances in which personal data and special category data can legitimately be shared without the knowledge of the individuals affected.

If it is identified that there is a need to systematically share personal data or special category data without the knowledge of the affected individuals, a Data Protection Impact Assessment (DPIA) must be completed prior to any information being shared. Partner organisations involved in such processing agree to provide all necessary assistance to one another to ensure that a DPIA is completed and that any resulting recommendations are implemented.

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 organisations will consider implementing local controls to identify such patterns of ad hoc behaviour

Where ad hoc sharing is required in circumstances that are not time dependent, partner organisations will ensure that requests are submitted in writing, containing a sufficient amount of detail to enable the receiving organisation to make a decision as to whether they are able to legitimately share the personal data.

Sharing in such circumstances is discretionary and each partner organisations acknowledges that the decision to share information sits solely with the receiving partner.

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. HSCN, PSN, CJX, Data Protection and Security Toolkit (DSPT). 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 partners shall have a security policy in place which sets out management commitment to information security, defines information security responsibilities, and ensures appropriate governance.

All staff must complete locally arranged data protection and information security training commensurate with their role and will be subject to pre-employment checks that take into account relevant employment legislation including verification of identity and right to work must be applied to all staff.

6.1.1. General

All partners shall have a security policy in place which sets out management commitment to information security, defines information security responsibilities, and ensures appropriate governance.

All staff must complete locally arranged data protection and information security training commensurate with their role and will be subject to pre-employment checks that take into account relevant employment legislation including verification of identity and right to work must be applied to all staff.

6.1.2. IT Infrastructure

Boundary Firewall and Internet Gateways **-** Information, applications and devices must be protected against unauthorised access and disclosure from the internet, using boundary firewalls, internet gateways or equivalent network devices.

Secure Configuration - ICT systems and devices must be configured to reduce the level of inherent vulnerabilities and provide only the services required to fulfil their role.

User Access Control - User accounts must be assigned to authorised individuals only, managed effectively, and they must provide the minimum level of access to applications, devices, networks, and data.

Access control (username & password) must be in place. A password policy must be in place which includes:

- Avoiding the use of weak or predictable passwords;
- Ensuring all default passwords are changed;
- Ensuring robust measures are in place to protect administrator passwords;
- Ensuring account lock out or throttling is in place to defend against automated guessing attacks.

End user activity must be auditable and include the identity of end-users who have accessed systems.

Malware Protection - Mechanisms to identify detect and respond to malware on ICT systems and devices must be in place and must be fully licensed, supported, and have all available updates applied.

Patch Management and Vulnerability Assessment - Updates and software patches must be applied in a controlled and timely manner and must be supported by patch management policies.

Partner organisations must adopt a method for gaining assurance in your organisation's vulnerability assessment and management processes, for example by undertaking regular penetration tests.

Software which is no longer supported must be removed from ICT systems and devices.

Backups and Recovery - ICT Systems processing personal data must be subject to operational procedures which support effective and secure backup. Backup arrangements must be regularly tested to ensure the process is successful and meets the requirements of the organisational policy.

Cloud Services – Partner organisations must ensure that the controls applied to the use of cloud services satisfactorily supports the relevant security principles set out in the National Cyber Security Centre Cloud Security Principles:

https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles

6.1.3. Protecting Data

International Transfers of Personal Data -In accordance with data protection legislation a transfer of personal data must be within the EU unless the rights of the individuals in respect of their personal data is protected in another way (subject to approval), or one of a limited number of exceptions applies.

Electronic Data - Electronic copies of data must be encrypted at rest to protect against unauthorised access. On portable devices e.g. laptops, netbooks, must be encrypted using AES 256 bit encryption.

When transmitting data over the internet, over a wireless communication network e.g. Wi-Fi, or over an untrusted network you must use an encrypted communication protocol.

Data transfer shall be achieved in a secure manner such as secure email (accredited to ISO27001:13); 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.

You must only use ICT which is under your governance and subject to the controls set out in organisational policy.

Hard Copy Data - Hard copy data must be stored securely when not in use and access to the data must be controlled.

It must be transported in a secure manner commensurate with the impact a compromise or loss of information would have and which reduces the risk of loss or theft.

6.1.4. Secure Destruction of Data

Electronic copies of data must be securely destroyed when no longer required. This includes data stored on servers, desktops, laptops or other hardware and media.

Hard copy data must be securely destroyed when no longer required.

Secure destruction means destroying data so it cannot be recovered or reconstituted.

A destruction certificate may be required to provide the necessary assurance that secure destruction has occurred.

6.1.5. Security Incidents/Personal Data Breach

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 governing information sharing agreement.

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

If a security incident or data breach cannot be resolved following intervention, sharing shall stop unless the risk of doing so is outweighed by the need to continue sharing. Authority to continue must come from the originating partner organisation and any breach notification must be advised ASAP to comply with the 72 hour reporting requirement.

6.1.6. Compliance

Partner organisations must be informed of any non-compliance with these controls. Any deficiencies in controls must be subject to a documented risk management process and where appropriate a remedial action plan is to be implemented with the aim of reducing, where possible, those deficiencies.

7. Individual Rights

The GDPR and the DPA 2018 gives individuals certain rights over their personal data.

These include:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

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 GDPR and DPA.

Individuals can object where the use of their personal data is causing them substantial, unwarranted damage or substantial, unwarranted distress however this 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 GDPR and DPA

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 lawful bases that are engaged and details of the supporting legal framework that legitimises 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 Protocol

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

Appendix A

Signatory: East Midlands Ambulance Service 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:	John Stephenson
Role:	Caldicott Guardian
Signature:	
Date:	25.2.2019

Each organisation is required to keep a copy of their signed agreement and send a scanned 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:	MARIE FOSH.
Role:	DIRECTOR OF WORKFORCE + TRANSFORMATION / DEPUTY CEO / SIRO
Signature:	
Date:	4. March 2019

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

13

Lincolnshire Inter-Agency Information Sharing Protocol V7

Signatory: Lincolnshire County Council

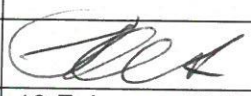
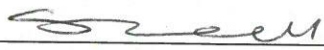
I (the Caldicott Guardian / SIRO) agree to support and implement the Lincolnshire Inter-Agency Information Sharing Protocol in order to facilitate appropriate and lawful sharing of information between the specified partner organisations.

Name:	Dr Kakoli Choudhury
Role:	Consultant in Public Health Medicine and Caldicott Guardian for Adult Care and Community Wellbeing
Signature:	
Date:	26.2.19

Each organisation is required to keep a copy of their signed agreement and send a scanned 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 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:	Tracy Pilcher SIRO	Sarah Southall Caldicott Guardian
Role:	Acting Accountable Officer	Acting Chief Nurse
Signatures:		
Date:	19 February 2019	

Each organisation is required to keep a copy of their signed agreement and send a scanned 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:	Sarah Connery
Role:	Senior Information Risk Owner
Signature:	
Date:	28.02.2019

Each organisation is required to keep a copy of their signed agreement and send a scanned 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:	ANDREW WHITE
Role:	ASSISTANT CHIEF OFFICER
Signature:	Andrew White
Date:	21/2/19

Each organisation is required to keep a copy of their signed agreement and send a scanned 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:	Jo Wright
Role:	Chief Finance Officer
Signature:	
Date:	12.03.19

Each organisation is required to keep a copy of their signed agreement and send a scanned 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:	Jo Wright
Role:	Chief Finance Officer
Signature:	
Date:	12.03.19

Each organisation is required to keep a copy of their signed agreement and send a scanned 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 West Clinical Commissioning Group

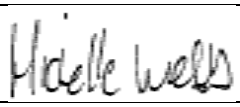
I (the Caldicott Guardian / SIRO) agree to support and implement the Lincolnshire Inter-Agency Information Sharing Protocol in order to facilitate appropriate and lawful sharing of information between the specified partner organisations.

Name:	Martin Bambro
Role:	Head of Performance/SIRO/IG Lead
Signature:	
Date:	20th February 2019

Each organisation is required to keep a copy of their signed agreement and send a scanned 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 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:	Michelle Webb
Role:	Director of Patient Care
Signature:	
Date:	11 2 2019

Each organisation is required to keep a copy of their signed agreement and send a scanned 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:	KEVIN TURNER
Role:	DEPUTY CEO
Signature:	
Date:	6 March 2019

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