

LINCOLNSHIRE COUNTY COUNCIL

**Information sharing agreement including:
Section 117 Mental Health Act Joint Policy and Procedures and Guidance**

Between the following partners:

**Lincolnshire County Council
and
NHS Lincolnshire Integrated Care Board
with
Lincolnshire Partnership NHS Foundation Trust**

Reference: 201920-033

Version 1.1

Document Control

Reference	Procedures and Guidance to the S117 MHA Joint Policy
Date	V1.0 12 December 2019 V1.1 1st December 2022
Author	Heston Hassett V1.1 Neil Chadwick
Date agreement comes into force	December 2019 V1.1 1 ST December 2022
Date of Agreement review (at least once every three years).	1 st December 2025. Please see 9.2 in respect of ad hoc reviews
DPIA Reference	LCC-DPIA-1920-033

Version History

Date	Version Number	Revision Notes	Author
4 th October 18	V0.1	Creation HH	Heston Hassett /Rebecca Bray
11 th October 19	V0.2	Comments from P&G group and LCCIG	Heston Hassett /Rebecca Bray
6 th November 19	V0.3	CCG comments	Lynn Wray
28 th November 19	V0.4	IG minor amendments	Heston Hassett /Rebecca Bray
10 th December 19	V0.5	Amendment based upon comments from LPFT and CCG IG lead	Heston Hassett /Rebecca Bray
12 th December 19	V1.0	Includes retention details and DPO contacts for each organisation	Heston Hassett
11 th October 22	V2.0	<ul style="list-style-type: none"> Amended Clinical Commissioning Group to Integrated Commissioning Board following organisational change. Adjusted numbering to link to respective policy and Procedure & Guidance. Increased the identification of legal documents in section 5.1. Included the sharing of information with the Quality Assurance groups at 5.4. Increased the review period from annually to once every three years. 	Neil Chadwick

1. Introduction

- 1.1 The purpose of this agreement is to document instances of systematic information sharing between Controllers. It assists in determining respective responsibilities for compliance with data protection legislation.
- 1.2 For the purposes of this Agreement, 'data protection legislation' means the General Data Protection Regulation ("GDPR") and the Data Protection Act 2018 ("DPA 2018").
- 1.3 The partnership organisations named in this ISA are all part of an agreed multi-agency S117 Mental Health Act Policy (Appendix C) and its associated Procedures and Guidance. This ISA is for the purpose of enabling the sharing of information for:
 - 1.3.1 Maintaining a 'S117 Master list' set in 3.3 S117 Mental Health Act Policy via the method set out in section 3.0 of the S117 Procedures and Guidance (Appendix D)
 - 1.3.2 To enable staff to share clinical information in determining an individual's S.117 needs.

2. Partners

2.1 The following Controllers are defined as Information Sharing Partners for the purpose of this agreement:

Lincolnshire County Council
NHS Lincolnshire Integrated Care Board
Lincolnshire Partnership NHS Foundation Trust

2.2 No changes to participating partners will be made without the consensus of the signatories to this agreement. Any such changes will be captured within an updated version of this agreement and circulated as soon as practicable to all partners.

3. Purpose of Sharing

3.1 This agreement is designed to facilitate the sharing of information between the partners listed above for the purpose of:

- Section 117(2) of the **Mental Health Act 1983** (as amended by 2007 MHA) puts a duty on Integrated Care Boards (ICB) and the Local Social Services Authority (LA) to provide, or to arrange for the provision of, aftercare services for patient who are eligible to be in receipt of such aftercare services identified in **Section 117(1) MHA**.
- It is a legal requirement that people eligible for S117 After care do not have to pay for those services.
- In addition, S75(1) of the **NHS Act 2006** allows ICBs and LAs to enter into arrangements for delivering aftercare services.
- The three partners in this agreement have created and approved for use a multi-agency S117 MHA Joint Policy (**Appendix C**). Which sets out at 3.3 the requirement of maintain a 'Section 117 Master list'.
- The S117 Joint Procedures and Guidance (**Annex D**) sets out a method for identifying, capturing, and sharing patient identifiable information between the organisation's. This data will in turn allow the partners in this agreement to meet their business requirements of:
 - 1) Ensuring only eligible individuals are identified as requiring S.117 aftercare.
 - 2) Ensuring eligible patients are not unlawfully charged for any S117 After care services that they are entitled to.
 - 3) Assist the CCG and LCC in their current and future aftercare provisions and planning.
 - 4) Providing details of detention, commencement & discharge, and where applicable the ending of S.117 aftercare eligibility.

4. The Sharing Process

4.1 **What:** The following information will be shared

The purpose of the S117 Policy and Procedures and Guidance is to ensure the departments responsible for funding S117 aftercare can readily identify eligible patients and to ensure eligible patients are not being charged for services unlawfully.

Only patients who are eligible for S117 of the MHA as set out in 1.1 of S117 Procedures and Guidance will be held on the S.117 Master list. The S.117 Master list will hold the following info which will be shared:

- Person Name
- DOB
- NHS Number and/or Mosaic Identity Number.

In addition to this the following information will be shared to determine an individual's after-care need, including Special Category data:

- Information about their health and wellbeing, and their day to day support needs.
- Information relevant to their cultural, spiritual or religious beliefs where we need to take these into account when providing support.
- Personal data relevant to the services they are currently receiving or have received in the past from health and social care.
- Information about family relationships and other members involved in your care and support.
- Details of any legal status and documents (e.g. section papers, transfer orders or court orders, immigration, Power of Attorney etc.)

4.2 **When:** The information will be shared:

With regards to the Master list the information will be shared on a monthly basis as set out in section 3 at 3.3 of the S117 Procedures and Guidance.

With regards to information needed to determine and individuals after-needs this will be done on an on-going basis.

4.3 **Who:** Partners must ensure that only those with a clear business requirement are able to access the shared personal data. The following restrictions apply:

The S117 Master list will be maintained by the MHA Office at Lincolnshire Partnership Trust. They will receive information from the bodies set out in the table at 1.2.2 of the S117 Procedures and Guidance.

The S117 Master list will then be provided to the Finance Team at Lincolnshire County Council and South West Lincolnshire Clinical Commissioning Group.

4.4 **How:** Partner agencies will share information by the following means:

With regards to the Master list

The secure Email addresses for each organisation are:

- CCG – licb.mhldateam@nhs.net
- LCC - AdultCareFinance@lincolnshire.gov.uk
- Gail.Kirk@lincolnshire.gov.uk
- LPFT MHA Office - lpft.MHA@nhs.net

Email with same Email domain

- Directly between nhs.net accounts
- Directly between lincolnshire.gov.uk accounts

Email sent between different domains

- lincolnshire.gov.uk sent to other domains must be Encrypted
- Security
- nhs.net sent to other domains must be password protected

With regards to assessing and care planning an individual person's after-care needs:

In addition to those named above information can be shared at MDT and Quality Assurance meetings and between professionals such as via phone, face to face meetings.

5. Governance

5.1 Any instance of systematic sharing must be compliant with current data protection legislation

5.2 Controllers are required to appropriately document their information sharing arrangements and the aim of this agreement is demonstrate and evidence the Controllers consideration of the key principles of data protection with regard to the purpose for which information is being shared (as set out paragraph 2 above)

5.3 Fair, Lawful and Transparent

5.3.1 The legal basis for sharing this information has been defined as:

Lincolnshire County Council and NHS Lincolnshire Integrated Care Board are relying on the below detailed lawful basis, relating to the detailed legislation with section 4.1;

- Article 6 (c) - Legal obligation - See 4.1 above
- Article 9 (h) - The collection of Health and Social Care
- Schedule 2 16 (1) (c) (ii) processing is necessary for the purposes of providing support for individual relating to a health condition.

Lincolnshire Partnership Foundation Trust are relying on the below detailed lawful basis, relating to the detailed legislation with section 4.1;

- Article 6 (b) contract (under S.75 contract and supported further by the specific contract commissioned jointly by Lincolnshire County Council and NHS Lincolnshire Integrated Care Board
- Article 9 (h) - The collection of Health and Social Care
- Schedule 2 16 (1) (c) (ii) processing is necessary for the purposes of providing support for individual relating to a health condition.

Information that will inform decision making of the identified partners of the ISA (listed in section 3.1) in the provisions of delivering and reviewing S117 aftercare. This in turn will allow the Lincolnshire County Council and NHS Lincolnshire Integrated Commissioning Board to accurately monitor individuals progress and the planning and costing of future provisions.

Individuals are provided with information advising them of what information will be shared in order to determine their needs via an information leaflet (detailed in Annex E)

5.3.2 Any information shared, and the processes used to share such information must be compliant with the relevant Human Rights legislation.

5.3.3 Each partner to this agreement undertakes to provide individuals with concise, accurate and easy to understand information about how their personal data will be used in relation to the purpose.

5.3.4 Each partner must ensure that privacy information is communicated in accordance with its own legal obligations.

5.4 Collected for specific, explicit and legitimate purposes

5.4.1 Partners undertake that information shared under this agreement will only be used for the specific purpose for which it was shared and in no circumstances will the information be processed further in a manner that is incompatible with the purpose as described in Para 2.

5.5 Adequate, relevant and limited to what is necessary

5.5.1 Each Partner undertakes that the information shared is the minimum amount of information required to achieve the purpose and the sharing of this information is necessary to meet the purpose.

5.6 Accurate and, where necessary, kept up to date

5.6.1 Each partner sharing information under this agreement is responsible for the quality of the information that it is sharing and must ensure it is accurate, relevant, and usable.

5.6.2 Before sharing information, staff will check that the information being shared is accurate and up to date to the best of their knowledge. If special categories of information are being shared which could harm the individual if it was inaccurate, then particular care must be taken.

5.6.3 Where a 'dataset' is being shared i.e., structured information, it will be accompanied by a table providing definitions of the data fields. This is summarised in Annex C.

5.6.4 Queries about the accuracy of information must be resolved by the partner supplying the information as soon as possible through the partners Single Point of Contact (SPOC).

5.7 Kept in a form which permits identification for no longer than is necessary

5.7.1 A set of retention schedules for information/records produced and received to support the operation of this Agreement is to be established.

5.7.2 Partners must try to establish and comply with a common set of retention schedules. It is accepted that partners may need to set their own retention periods because of different statutory requirements. However, in all cases when organisational retention periods expire and there is no longer a business requirement to hold the information it must be securely deleted.

5.7.3 The agreed retention schedule for this Agreement is provided below:

Lincolnshire County Council retention Schedules
NHS Lincolnshire Integrated Care Board retention Schedules
Lincolnshire Partnership Foundation Trust retention Schedules

5.8 Security

5.8.1 Information must be kept secure when it is being shared, handled and at rest. It is therefore necessary to agree common security practices between partners. For the purpose of this agreement Annex B sets out the minimum information security controls that all partners agree to abide by. [These standards are to be agreed by all parties - where they cannot be met amendments must also be agreed by all parties]

6. Individual Rights

6.1 Data protection legislation gives individuals certain rights over their personal data. These include:

- The right to access personal data held about them
- The right to withdraw consent.
- The right to request that inaccurate data is rectified, and incomplete data is completed
- The right to request erasure of data
- The right to request restriction of processing
- The right to data portability
- The right to object to decisions made on the basis of automated processing and/or profiling.

6.2 Partners are responsible for ensuring they have supporting policies- and procedures in place to support individual rights.

7. Single Point of Contact (SPOC)

7.1 All partners to this agreement must appoint a SPOC

7.2 Any person who is unclear about any aspect of this agreement must contact their SPOC in the first instance.

7.3 The following SPOCs have been identified for each partner:

Lincolnshire County Council Justin Hackney, Assistant Director Specialist Adult Services and Safeguarding, Adult Care and Community Wellbeing
NHS Lincolnshire Integrated Care Board Matt Gaunt Director of finance
Lincolnshire Partnership NHS Foundation Trust Mark Platts Director of Finance and Information

7.4 The DPOs have been identified for each partner:

following

Lincolnshire County Council Amy Jaines DPO@lincolnshire.gov.uk
NHS Lincolnshire Integrated Care Board Judith Jordan agem.dpo@nhs.net
Lincolnshire Partnership NHS Foundation Trust Dawn Selkirk d.selkirk@nhs.net

8. Review

8.1 This agreement will be reviewed as a part of the on-going Governance and review of the S117 Joint Mental Health Act Policy and its Procedures and Guidance.

8.2 If a significant change takes place which means that the agreement becomes an unreliable reference point, then the agreement will be updated as needed and a new version circulated.

8.3 The review must ensure the agreement remains fit for purpose and that safeguards remain relevant and appropriate.

9. Signatories

9.1 By signing this agreement, all signatories accept responsibility for its execution and agree to the conditions set within.


9.1.1 Lincolnshire County Council

Signed on behalf of **Lincolnshire County Council:**

Name: Justin Hackney

Position: Assistant Director Specialist Adult Services and Safeguarding, Adult Care and Community Wellbeing Adult Services

Date: 13-10-2022

Signed: 

9.1.2 NHS Lincolnshire Integrated Care Board

Signed on behalf of **NHS Lincolnshire Integrated Care Board:**

Name: Matt Gaunt

Position: Director of Finance

Date: 01.11.22

Signed: 

9.1.3 NHS Lincolnshire Partnership Foundation Trust

Signed on behalf of **NHS Lincolnshire Partnership Foundation Trust:**

Name: Mark Platts

Position: Director of Finance and Information

Date: 21/11/2022

Signed: 

10. Appendices

10.1 Annex A – Glossary of Terms

Controller - a person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Subject - person who can be identified from the data

Personal Data - information relating to an identified or identifiable natural person, whether directly or indirectly, and with particular reference to identification by name, identification number, location data, online identifiers or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Processor - any person (other than an employee of the controller) who processes the data on behalf of the controller

Special Categories of Personal Data - personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, a person's sex life or sexual orientation.

10.2 Annex B – Minimum Information Security Controls

General

A security policy must be in place which sets out management commitment to information security, defines information security responsibilities and ensures appropriate governance.

All staff must complete data protection and information security training commensurate with their role.

Pre-employment checks that take into account relevant employment legislation including verification of identity and right to work must be applied to all staff

IT Infrastructure

Boundary firewall and internet gateways

Information, applications and devices must be protected against unauthorised access and disclosure from the internet, using boundary fire walls, 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 the 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.

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

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

Cloud Services

You 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>

Protecting Confidential Data

Electronic Data

Electronic copies of confidential data must be encrypted at rest to protect against unauthorised access.

When transmitting confidential 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.

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

Hard Copy Confidential Data

Hard copy Confidential 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.

Secure Destruction of Confidential Data

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

Hard copy information 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.

Security Incidents/Personal Data Breach

You must notify the partners in this ISA immediately of any fact or event which results in, or has the potential to result in, the compromise, misuse, or loss of information identified in this ISA, ICT services or assets.

You must notify the partners in this ISA of any personal data breach if the breach relates to personal data processed on behalf of the partners in this ISA. .

You must fully co-operate with any investigation that the partners in this ISA require as a result of such a security incident or personal data breach.





Compliance

The partners in this ISA 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.

Independent validation which has been used as evidence of appropriate security controls must be maintained throughout the life of the contract.

The partners in this ISA must be made aware of any expired or revoked evidence used as independent validation.

10.3 Annex C – G – Embedded Documentation

<p>Annex C S117 Mental Health Act Joint Policy</p>	 S117 Joint Policy v4 2022 DRAFT (010) 21
<p>Annex D Procedures and guidance for the Section 117 aftercare</p>	 Procedures and Guidance V1.9a (for
<p>Annex E Lincolnshire County Council – Adult Care and Community Wellbeing assessment and support privacy notice</p>	 Privacy-Notice---Ad ult-Care-and-Comm
<p>Annex F NHS Corporate records, retention and disposal schedule and guidance</p>	 B1785-nhse-corpor ate-records-retentio
<p>Annex G Code of practice for handling information in health and Social Care – NHS Digital</p>	Code of Practice NHS Digital LINK