

**Information Sharing Agreement between Nottinghamshire
Healthcare NHS Foundation Trust (NHCFT) & All partner
agencies named in the agreement**

Title:	<p>Information Sharing Agreement (ISA) between Nottinghamshire Healthcare NHS Foundation Trust (NHCFT),</p> <p align="center">&</p> <p>Nottingham City Council - www.nottinghamcity.gov.uk</p> <p>Nottinghamshire County Council – www.nottinghamshire.gov.uk</p> <p>Nottingham City Housing Association/Metropolitan - www.ncha.org.uk / www.metropolitan.org.uk</p> <p>Change Grow Live - www.changegrowlive.org</p> <p>'HIMMAH' – People's Pantry - www.himmah.co.uk/npp</p> <p>Mansfield Community Voluntary Service - www.mansfieldcvs.org</p> <p>Framework - www.frameworkha.org</p> <p>Age UK Notts - www.ageuk.org.uk/notts/</p> <p>POhWER - www.pohwer.net</p> <p>Improving Lives - www.improvinglivesnotts.org.uk</p> <p>Opportunity Nottingham - http://www.opportunitynottingham.co.uk/</p> <p>MIND - www.mind.org.uk</p>
Author/Contributor	<p>Author – Laura Baker, Information Assurance Officer</p> <p>Contributors – Sandra Crawford, Winter Pressures Project Manager & all Signatory Organisations</p>
Approved By:	<p>Data Protection Officer and Caldicott Guardian of NHCFT and Caldicott Guardian or equivalent of other organisations</p>
Approval Date:	<p align="center">May 2021</p>
Method of Dissemination:	<p>By Heads of Service/Team Managers within all organisations</p>

Dissemination Date:	May 2021
Implementation Date:	May 2021
Review Date:	April 2022

Document History

Version No.	Date	Brief Description
0.1		Draft of Information (Data) Sharing Agreement.

Contents

1. Introduction	4
2. Purpose of sharing the information	4
3. Information being shared.....	4
4. Legal basis of sharing information	4
5. Organisations involved in the data sharing	5
6. When information will be shared	5
7. Data Quality	5
8. Retention of data	5
9. Security of information	6
10. Access to information	8
11. Compliance with the agreement.....	8
12. Indemnity.....	8
13. Monitoring and review.....	8
14. Termination of the agreement	8
Appendix A - Terms of Agreement and Signatures	9
8.1 Declaration:.....	9
Appendix A. Signatory Sheet - Information Sharing Agreement.....	10
Appendix B – Data being shared	12
Personal data [Person Identifiable Data (PID) / Personal Identifiable Information (PII)]	12
Appendix C - Key Legislation / Best Practice Guidelines	12
Access to Health Records Act 1990.....	12
General Data Protection Regulation 2016/679 and Data Protection Act 2018.....	13
The Caldicott Principles.....	14
The Crime and Disorder Act 1998	14
Human Rights Act 1998.....	14
Freedom of Information Act 2000	14
General Power of Competence – Localism Act 2011	15
The Common Law Duty of Confidentiality	15
Other Relevant Legislation.....	15
There are statutory restrictions on passing on information linked to:	16

1. Introduction

This Information Sharing Agreement (ISA) sets out how information will be shared between the parties to the agreement. The Agreement aims to ensure compliance with the relevant legislation and the statutory revised (2020) ICO Data Sharing Code of Practice; <https://ico.org.uk/for-organisations/data-sharing-a-code-of-practice/>

Whilst the over-riding benefits of sharing are recognised in the public community there is also an expectation to ensure only the minimum necessary amount of Personal Data is shared, with the right partners, at the right time and for the right reasons in accordance with the principles of Data Protection Act (DPA) 2018 and the General Data Protection Regulation (GDPR) 2016/679.

The information to be shared and the circumstances in which it will be shared are described in section 3.

2. Purpose of sharing the information

The purpose of sharing information between the signatory organisations:

Nottinghamshire Healthcare NHS Foundation Trust (NHCFT) have been allocated additional funding to support mental health patients initially during the winter 2020/2021, but this has now been extended throughout this year until March 2022. This will be used to improve their journey through in-patient services and increase community support that they may need upon discharge. Patients needing additional support during and after the discharge process will be identified and referrals will be made to the relevant parties named in this document.

3. Information being shared

The type of information which will be shared includes:

Patient Name
RiO Number
DOB
Address
NHS number
Gender
Ethnicity
Relevant referral information relating to the patients' needs

4. Legal basis of sharing information

The legal basis for sharing information is set out below:

All organisations agree to comply with the Human Rights Act 1998 (HRA) in the performance of their functions and the six principles of the Data Protection Act (DPA) 2018. Conditions currently under Schedules 2 and 3 of the Data Protection Act 2018 will be met which 'allows the lawful processing of information, taking into account the common law duty of confidentiality.'

Conditions from Article 6, 1(a) will be met; 'the data subject has given consent to the processing for one or more purposes.

Conditions from Article 9 of the UK GDPR will be met; 'processing is necessary for the purpose of the provision of health or social care or treatment, or the management of healthcare systems.' Meeting the conditions of the Common Law Duty of Confidentiality in regard to explicit consent.

All parties also agree to adhere to the Information Commissioner's (ICO) Data Sharing Code of Practice, using this as a framework to make good quality decisions about information sharing.

5. Organisations involved in the data sharing

Information will be shared when appropriate between the parties listed in the signatories' section. A ppendix [A].

6. When information will be shared

Under the terms of this agreement information should be shared:

To ensure timely patient care, information will be shared from NHCFT to the relevant parties at the point of referral via one of the following methods; Paper referral form if this is the usual referral method as agreed by NHCFT and the relevant organisation(s).
Electronic referral if this is the usual referral method agreed by NHCFT and the relevant organisation(s)

Some individuals from the named organisations have honorary contracts with NHCFT which include being able to access the RiO patient electronic system. In these cases, relevant information relating to the referral may also be shared via this method.

7. Data Quality

All parties will ensure the data being shared is accurate so that any decisions taken regarding patient care are based on up to date and accurate information. NHCFT requires that all partner organisations party to this agreement meet the data quality processes as defined in the Trust Information Assurance Framework.

8. Retention of data

Data will be retained by the parties named in this agreement as follows:

The data will be retained in line with each organisation's retention policies and the Records Management Code of Practice for Health and Social care 2016.

9. Security of information

All parties must put in place adequate precautions to ensure the security of information being shared. All parties must have completed a submission to the NHS Data Security and Protection Toolkit on all requirements or have appropriate approved action plans in place.

All parties have agreed that the following measures are required and have been implemented:

Information Security Assurance

- Monitoring and enforcement processes are in place within all parties to ensure compliance with NHS national information security standards.
- Operating and application information systems used by all parties to process the shared data support appropriate access control functionality and documented and managed access rights are in place for all users of these systems.
- Policies and procedures for all parties ensure that all end point devices are secure.
- All parties will maintain an information asset register that includes all key information, software, hardware and services.
- All parties have documented and embedded plans and procedures to support business continuity in the event of power failures, system failures, natural disasters and other disruptions.
- All parties have documented incident management and reporting procedures.
- All parties will ensure any and all transfers of hardcopy and digital personal and sensitive information are identified, mapped and risk assessed and that technical and organisational measures adequately secure these transfers.
- All parties confirm that all information assets that process personal data are protected by appropriate security measures.
- All electronic correspondence containing sensitive and/or confidential information which requires transfer between any of the parties will be sent via secure NHS Mail or some other mail system that conforms to the ISB1596 NHS Secure Email standard¹.

Clinical Information Assurance

- Procedures are in place to ensure the accuracy of service user information on all systems and /or records that support the provision of care.

¹ <https://digital.nhs.uk/services/nhsmail/the-secure-email-standard>

Security of Information - General

- All parties will maintain appropriate confidentiality, information security, data protection and records management policies.
- Each party is responsible for ensuring the security of the information held on its own systems and premises and for reporting, investigating and resolving any security breaches in line with internal policies and procedures.
- Each party will manage any incidents or activities that suggest non-compliance with any of the terms of this ISA in accordance with the NHS serious incident framework and ICO requirements. This includes, where appropriate, 'near miss' situations even if no actual damage to or loss or inappropriate disclosure of the information results.
- No party should share, disclose or otherwise reveal the information (in whole or in part) for which NHCFT is the Data Controller to any individual, business or other organisation who is not a party to this agreement without the explicit written consent of NHCFT, other than in compliance with a statutory obligation or as a result of a Court order or another legal basis.

Security of Information – Physical

- All parties will ensure that information is physically protected from potential damage arising from environmental hazards such as fire and flood.
- All parties will ensure that the information is held on premises that are adequately protected from unauthorised entry and/or theft.

Security of Information - IT Systems

- All parties will only hold the information in accordance with Department of Health policy and on secure servers, not on portable media or devices such as laptops or USB memory sticks or CD-ROMs or employees' own personal computers.
- All parties will ensure adequate back-up facilities to minimise the risk of loss of or damage to the information and that a robust business continuity plan is in place in the event of restriction of service for any reason.
- All parties will only transmit information by the secure methods, whether it is in physical form or electronic transfer, using encryption.

Security of Information - Employees

- All parties will undertake all reasonable pre-employment checks to verify the identity, honesty, trustworthiness and general suitability of employees (including DBS checks where appropriate).
- All parties will include appropriate confidentiality clauses in employment contracts and reference will be made in relation to potential sanction action(s) which may be taken against any employee acting in a deliberate or reckless manner that breaches confidentiality or the non-disclosure provisions of Data Protection Act or causes damage to or loss of the information.

10. Access to information

Any requests for information received by any party to this agreement relating to data held by that party for which they are not the Data Controller, will be referred back to the Data Controller. For the purposes of this agreement the Data Controller for the information being shared with the named parties are NHCFT.

No party will share information for which they are not the Data Controller with any individual or organization which is not a signatory to this agreement without the prior agreement of the Data Controller, other than where such disclosure is required to comply with a statutory obligation or as a result of a Court order or another legal basis.

11. Compliance with the agreement

Any single major failure to abide by the conditions set out in this ISA or repeated non-compliance by a party will result in the termination of this ISA between that party and the other parties and the non-compliant party will not receive any further information under the terms of this agreement.

Where a party withdraws or are excluded from the agreement, the list of signatories must be updated to reflect the change.

No additional parties can be added to this agreement.

12. Indemnity

In the event that a party to this agreement discloses inaccurate information which subsequently incurs liability, cost or expense, the disclosing party should indemnify the requesting party or parties against liability, cost or expense incurred.

This indemnity, however, should not apply in cases where the requesting party was negligent in the use of received information, makes an admission that may prejudice [defense](#) of the action, claim or demand, or reaches a settlement with the disclosing party.

13. Monitoring and review

All parties to this ISA will monitor any breaches or problems in relation to this agreement within their own organisation.

A review of the ISA will take place as per the review date on the opening page of this ISA, unless legislative changes require immediate action or at the request of any signatory.

14. Termination of the agreement

On termination of the agreement by any party, information in the possession of the terminating party will be securely destroyed as per their records management policy.

Appendix A - Terms of Agreement and Signatures

The agreement should be signed by any two of the following three designated persons within NHCFT:

Caldicott Guardian, Data Protection Officer or Senior Information Risk Owner (SIRO)

and a designated person from each participating organisation, such as:

a Caldicott Guardian (for Health & Social Care related data), a SIRO, a person designated by a Caldicott Guardian, SIRO or the business manager responsible for the data being shared.

8.1 Declaration:

I, the undersigned, on behalf of my organisation named below, agree to support the implementation and operation of this ISA in accordance with the conditions detailed in this document, including the resolution of any action points arising. I also understand that my organisation may share information with other parties listed as signatories to this agreement.

8.2 As part of this undertaking my organisation will operate in accordance with the law and agree to abide by this ISA.

8.2.1 My organisation has organisational and technical measures in place, with relevant supporting operational protocols, policies and procedures.

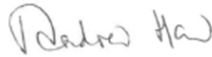
8.2.2 All Person Identifiable Data / Person Identifiable Information will be managed and secured in accordance with the law, including the method of transmission used to transmit data.

8.2.3 Information will be destroyed in accordance with the policies and procedures of my organisation once it has fulfilled its purpose and is no longer needed.

8.2.4 All information shared will be used in accordance with this ISA.

8.2.5 Recipients of information from all parties will ensure that it is received and handled only by those authorised (and trained) to handle the information, throughout the lifecycle of the information.

Appendix A. Signatory Sheet - Information Sharing Agreement

Organisation	Name	Position	Signature	Date
Nottinghamshire Healthcare NHS Foundation Trust	Dr Susan Elcock	Executive Medical Director and Caldicott Guardian		
Nottinghamshire Healthcare NHS Foundation Trust	Andrew Haw	Data Protection Officer		<u>8 July 2021</u>
Nottingham City Council				
Nottinghamshire County Council				
Nottingham City Housing Association				
Change Grow Live				
HIMMAH – People’s Pantry	Sajid Mohammed			
Mansfield Community Voluntary Service	Steve Morris	Chief Executive officer		
Framework				

Age UK Notts	Di Trinder	Joint Chief Executive	<i>DeLah.</i>	6/9/2021
POhWER				
Improving Lives	Kerry Devine	Interim CEO		
Opportunity Nottingham				
MIND	Nic Roberts	Chief Executive Officer		

Appendix B – Data being shared

Personal data [Person Identifiable Data (PID) / Personal Identifiable Information (PII)]

Information sufficient to identify a living individual by itself or in conjunction with other information. Includes any expression of opinion about an individual and any indication of the intentions by any person in respect of the individual. Please see Section 3 for specific information being shared.

Special Category Data

Special category data is personal data which the GDPR says is more sensitive, and so needs more protection. Special Category data includes data relating to:

- Race
- Ethnic Origin
- Politics
- Religion
- Trade Union Membership
- Genetics
- Biometrics (where used for ID purposes)
- Health
- Sex Life or
- Sexual orientation

Appendix C - Key Legislation / Best Practice Guidelines

All parties to this ISA are subject to a variety of legal, statutory and other good practice guidance in relation to the sharing of person-identifiable or anonymised information.

For all partners the key legislation and guidance affecting the sharing and disclosure of information includes (not exhaustive):

- Access to Health Records 1990*
- Data Protection Act 2018*
- Crime and Disorder Act 1998
- Human Rights Act 1998*
- Freedom of Information Act 2000*
- Safeguarding Vulnerable Groups Act 2006
- Education Act 2002
- Mental Capacity Act 2005
- Local Government Act 2000*
- General Data Protection Regulation 2016/679
- Caldicott Principles

*Additional information for some of the above is given below:

Access to Health Records Act 1990

This Act provides rights of access to the health records of deceased individuals for their

personal representatives and others having a claim on the deceased's estate.

In other circumstances, disclosure of health records relating to the deceased should satisfy common law duty of confidence requirements. The Data Protection Act 2018 supersedes the Access to Health Records Act 1990 apart from the sections dealing with access to information about the deceased.

General Data Protection Regulation 2016/679 and Data Protection Act 2018

The key legislation governing the protection and use of identifiable patient/client information (Personal Data) is the General Data Protection Regulation (GDPR) 2016/679 and the Data Protection Act (DPA) 2018.

Both the GDPR and DPA give rights to individuals in respect of their own personal data held by others:

- 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

In addition, the GDPR and DPA stipulate that anyone processing personal data must comply with seven principles of good practice. These principles are legally enforceable:

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality (security)
7. Accountability

The risks to sensitive, confidential information include (but are not limited to) accidental or unauthorised access to, or destruction, loss, use, modification or disclosure of, personal data.

There is no principle for individuals' rights. This is now dealt with separately in Chapter III of the GDPR; *Rights of the Data Subject*.

There is no principle for international transfers of personal data. This is now dealt with separately in Chapter V of the GDPR; *Transfers of Personal Data to Third Countries or International Organisations*, and:

There is a new accountability principle; this specifically requires the Data Controller to take responsibility for complying with the principles, and to have appropriate processes and records in place to demonstrate that they comply.

The Caldicott Principles

The Caldicott Principles were developed in 1997 following a review of how patient information was handled across the NHS.

The Review Panel set out six Principles that organisations should follow to ensure that information that can identify a patient is protected and only used when it is appropriate to do so.

In April 2013 a review introduced an additional Caldicott Principle. The seven Caldicott principles are as below:

- Principle 1 Justify the purpose(s) for using confidential information
- Principle 2 Don't use personal confidential data unless it is absolutely necessary
- Principle 3 Use the minimum necessary personal confidential data
- Principle 4 Access to personal confidential data should be on a strict need-to-know basis
- Principle 5 Everyone with access to personal confidential data should be aware of their responsibilities
- Principle 6 Comply with the law
- Principle 7 The duty to share information can be as important as the duty to protect patient confidentiality

The Crime and Disorder Act 1998

Section 115 of the Crime and Disorder Act provides a power to exchange certain information between partners where the disclosure of information is necessary to support the overall **public protection service** (e.g. a local community safety strategy) or other provisions in the Crime and Disorder Act.

This power does not affect other legal obligations and means that the Data Protection Act, Human Rights Act and Common Law Duty of Confidentiality must still be adhered to.

Human Rights Act 1998

Public authorities must comply with the Human Rights Act 1998 (HRA) in the performance of their functions. The HRA also applies to organisations in the private sector insofar as they carry out functions of a public nature.

Where the HRA applies, organisations must not act in a way that would be incompatible with rights under the European Convention on Human Rights. It is important to ensure that rights to privacy are maintained and only over-riden in circumstances where it is judged the sharing of PID/PII is in the interests of public (e.g. public safety - it is used to prevent crime and disorder)

Freedom of Information Act 2000

This Act provides clear statutory rights for those requesting information together with a strong enforcement regime.

Under the terms of the Act, any member of the public is able to apply for access to information held by bodies across the public sector. The release of 'personal information' remains protected by the Data Protection Act 2018.

General Power of Competence – Localism Act 2011

The general power of competence under the Localism Act 2011 came into force on 18 February 2012. Local Authorities are now specifically empowered to do anything not prohibited by legislation, and subject to public law principles, they have the power to do anything that individuals generally may do.

Specifically, Section 1 of the Localism Act provides:

"A local authority has power to do anything that individuals generally may do "even if:

- it is unlike anything else the authority may do.
- it is unlike anything that other public bodies may do.
- it is carried out in any way whatever, including:
 - anywhere in the UK or elsewhere;
 - for a commercial purpose or otherwise for a charge, or without charge;
 - For, or otherwise than for, the benefit of the authority, its area or persons resident or present in its area.

The Common Law Duty of Confidentiality

Information will be regarded as confidential where it is reasonable to assume that the provider of the information expected it to be kept confidential.

A duty of confidence is characteristic of several types of relationship such as medical (doctor/patient), legal (solicitor/client) and caring (counsellor/client). However, a duty of confidence does not necessarily arise just because a document is marked "confidential", although such a marking may be indicative of an expectation of confidentiality.

The common law duty of confidentiality refers to Person Identifiable Data / Person Identifiable Information and means that individuals should be asked for permission to use their information or records prior to disclosure.

However, where an individual's consent cannot be obtained, designated officers are required to assess the case and decide whether or not disclosure is necessary to support the **public protection service** and therefore an over-riding public interest to do so including whether the duty of confidence should be over-ridden.

Person Identifiable Data / Person Identifiable Information can be disclosed without consent where it can be demonstrated that one or more of the following apply:

- Disclosure is required by law.
- There is a public interest.
- There is a risk of death or serious harm.
- Information will allow detection, prevention and prosecution of serious offences.
- It is in the interest of public health.
- It is in the interests of the individual's health.
- It is in the interests of the individual concerned.

Other Relevant Legislation

- Criminal Procedures and Investigations Act 1996
- Regulation of Investigatory Powers Act 2000

- Health and Social Care Act 2011 (Section 60)
- Homelessness Act 2002
- Information Commissioner's Office Data Sharing Code of Practice 2011

There are statutory restrictions on passing on information linked to:

- NHS (Venereal Disease) Regulations 1974
- Human Fertilization and Embryology Act 1990
- Abortion Regulations 1991

Best Practice Guidelines Documentation

- NICE and Transforming Care Plans
- 'Transforming Care, A National Response to Winterbourne View Hospital'. Final Report, Department of Health Review, December 2012.
- The Mental Health Act 1983 Code of Practice, (Presented to Parliament pursuant to section 118 of the Mental Health Act 1983). Department of Health TSO 2015.
- The Mental Health Act 2005, Code of Practice. Issued by the Lord Chancellor on 23 April in accordance with sections 42 and 43 of the Act, London, TSO 2007.
- 'Equality for All: Mental Health Act 1983: Code of Practice 2015: Equity Analysis'. Department of Health, 2015.
- 'Stronger Code: Better Care: Government Response to the Consultation on the Mental Health Act 1983: Code of Practice'. Department of Health 2015.
- The Mental Capacity Act in relation to Deprivation of Liberty and Safeguarding Valuing People: A New Strategy for Learning Disability for the 21st Century. Department of Health, White Paper. March 2001.
- Valuing People Now: a new three-year strategy for people with learning disability. 'Making it happen for everyone'. HM Government, January 2009.
- 'Death by Indifference: Following up the Treat me right! report'. Mencap. 2007.
- 'Healthcare for All: Report of the Independent Inquiry into Access to Healthcare for People with Learning Disabilities'. Sir Jonathan Michael. July 2008.
- 'Six lives: the provision of public services to people with learning disabilities'. Health Ombudsman. 2009.
- 'Services for people with learning disability and challenging behaviour or mental health needs' (The Mansell Report) (revised edition 2007).
- Valuing Employment Now (2009)
- Equal access? A practical guide for the NHS: creating a Single Equality Scheme that includes improving access for people with learning disabilities (2009)
- Improving the health and wellbeing of people with learning disabilities (2009)
- The Care Quality Commission indicator on Access to healthcare for people with LD for acute and specialist trusts
- The National report for commissioning services and support for people with learning disabilities and complex needs joint review (2009) published by The Healthcare Commission, Commission for Social Care Inspection and Mental Health Act Commission