positive about integrated healthcare

Nottinghamshire Healthcar
NHS Foundation Tru

Data Sharing Agreement between Nottinghamshire Healthcare (NHS) Foundation Trust (NHCFT), Nottinghamshire Social Care, Age UK Connect and Mansfield District Council

Title:	Data Sharing Agreement between Nottinghamshire Healthcare NHS Foundation Trust, Nottinghamshire Social Care, Age UK Connect, Mansfield District Council and Ashfield District Council
Author/Contributor	Author – Angela Peggs Nottinghamshire Healthcare NHS Foundation Trust Contributors - All signatory Organisations
Contact details	Angela Peggs Information Assurance Manager NHCFT Birch House Ransom Wood Business Park Mansfield NG21 0HJ Tel: 01159691300 Ext 13171 angela.peggs@nottshc.nhs.uk Elizabeth Barker Integrated Care Team Leader NHCFT elizabeth.barker@nottshc.nhs.uk Lisa Matthews Team Manager – Ashfield Mansfield Older Adults Community Assessment Team Nottinghamshire County Council lisa.matthews@nottscc.gov.uk Tracy Styles ASSIST Team Leader tstyles@mansfield.gov.uk Jackie McGuiness Age UK Connect Manager jackie.mcguinness@ageuknotts.org.uk
Approved By:	Data Protection Officer and Caldicott Guardian of NHCFT and Caldicott Guardian or equivalent of other organisations
Approval Date:	September 2019
Method of Dissemination:	By Heads of Service/Team Managers within all organisations
Dissemination Date:	September 2019
Implementation Date:	September 2019
Review Date:	September 2021

Document History

Version No.	Date	Brief Description
0.1		Draft of Information (Data) Sharing Agreement.
0.2		Draft incorporating comments from EB - NHCFT

Contents

1. Introduction

This Data Sharing Agreement (DSA) sets out how information will be shared between signatories to the agreement. The Agreement aims to ensure compliance with the relevant legislation and the statutory Data Sharing Code of Practice: https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf

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 Person Identifiable Data (PID) or Personal Identifiable Information (PII) 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:

For all organisations involved in this agreement to work together, to provide direct care and support for patients within the Local Integrated Care Teams service within NHCFT.

3. Information being shared

The type of information which will be shared includes:

NHS Number
Patient name
Date of Birth
Address
GP Surgery
Medical information
Social/family issues
Patient environmental information

During the meeting, discussions are held and outcomes are recorded directly into the patient's record by NHCFT and Social Care, if patient is known to them. Information shared verbally during the meeting includes medical information, social/family issues and the patient's environment.

Referrals are sent securely from NHCFT via email to AGE UK Connect using NHS Net accounts.

Any information shared between the organisations that is not required for on-going patient care will be confidentially destroyed after the weekly meeting.

System/Access to Information

There will be no access to each-other's systems by any of the organisations.

Any relevant patient information shared for direct care will be shared either verbally in the weekly MDT meeting attended by all organisations named within this agreement, or via secure email as a password protected document. The password will be relayed securely via another means, for example via telephone, not via email.

4. Legal basis of sharing information

The legal basis for sharing information is set out below:

Both organisations agree to comply with the Human Rights Act 1998 (HRA) in the performance of their functions and the principles of the Data Protection Act (DPA) 2018. Currently meeting conditions under chapter 2, Sections 8 and 11 of the DPA, allowing for lawful processing of information, taking into account the common law duty of confidentiality:

Under General Data Protection Regulation (EU) 2016/679 (GDPR) conditions under Articles 6 and 9 will be met: Article 6 (e); '*processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.*' Article 9.2.h: '*processing is necessary for the purposes of provision of health or social care or treatment or the management of health or social care systems.*'

Section 11 of the DPA 2018 Special categories of personal data etc: supplementary,:

(a)by or under the responsibility of a health professional or a social work professional

Note that this DSA does not propose to support the sharing of data about criminal convictions or offences.

All organisations agree to adhere to the Information Commissioners Office (ICO) Data Sharing Code of Practice, using this as a framework to make good quality decisions about information sharing.

All organisations agree to comply with the Human Rights Act 1998 (HRA) in the performance of their functions and the principles of the Data Protection Act 2018 and the General Data Protection Regulation (EU) 2016/679 (GDPR) conditions.

5. Organisations involved in the data sharing

Information will be shared between the organisations listed in section 3, see also the signatories section in Appendix [A].

6. When information will be shared

Under the terms of this agreement information should be shared:

Only for the purpose described in section 2 of this agreement.

7. Data Quality

Partners will ensure data being shared is accurate so that any decisions taken regarding service development and evaluation are based on accurate information.

8. Retention of data

Data will be retained by partners as follows:

The data will be retained in line with each organisation's retention policies. NHCFT will retain patient information in line with the Records Management Code of Practice for Health and Social Care 2016. Any patient information shared between the organisations that is either discussed at the weekly LICT MDT meeting or sent via secure email that is deemed as not required for the ongoing care of patients, will be deleted/confidentially destroyed within a week of the meeting taking place by each third party organisation.

9. Security of information

All partners 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.

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

Information Security Assurance

- Monitoring and enforcement processes are in place to ensure NHS national information security processes comply with the terms and conditions of use.
- Operating and application information systems used to manage this data (under each organisation's control) support appropriate access control functionality and documented and managed access rights are in place for all users of these systems.
- Policy and procedures ensure that all end point devices are secure.
- There is an information asset register that includes all key information, software, hardware and services.
- There are documented plans and procedures to support business continuity in the event of power failures, system failures, natural disasters and other disruptions.
- There are documented incident management and reporting procedures.
- All transfers of hardcopy and digital personal and sensitive information have been identified, mapped and risk assessed; technical and organisational measures adequately secure these transfers.
- All information assets that hold, or are, personal data are protected by appropriate security measures.
- Any correspondence containing patient information is transferred electronically between NHCFT and the 5 other organisations via secure NHS Mail or some other mail system that conforms to the ISB1596 NHS Secure Email standard[1].

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.

Security of Information - General

- Each of the parties will maintain appropriate confidentiality, information security, data protection and records management policies.
- Each of the parties 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 of the parties will manage any incidents or activities that suggest non-compliance with any of the terms of this DSA in accordance with the NHS serious

[1] https://digital.nhs.uk/services/nhsmail/the-secure-email-standard

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.

- The external organisations must not share, disclose or otherwise reveal the information (in whole or in part) to any individual, business or other organisation not directly involved in the delivery of this service without the explicit written consent of Nottinghamshire Healthcare NHS Foundation Trust, other than in compliance with a statutory obligation or as a result of a Court order or another legal basis.

- The external organisations will notify Nottinghamshire Healthcare NHS Foundation Trust of all staff that require access to the system and ensure that access is limited to those who have a need to know.

Security of Information – Physical

- Each of the parties will ensure that the information is physically protected from potential damage arising from environmental hazards such as fire and flood.

- Each of the 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

- Each of the 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.

- Each of the 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.

- Each of the parties will only transmit information by the secure methods, whether it is in physical form or electronic transfer, using encryption.

Security of Information - Employees

- Each of the parties will undertake all reasonable pre-employment checks to verify the identity, honesty, trustworthiness and general suitability of employees (including DBS checks where appropriate).

- Each of the parties will include appropriate confidentiality clauses in employment contracts, including details of sanctions 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

No information will be divulged to any third party other than in compliance with a statutory obligation or as a result of a Court order or another legal basis. Any requests for information

received by the external organisations about information they are holding, but for which they are not the Data Controller, will be referred back to the partner who provided it (NHCFT).

11. Compliance with the agreement

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

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

No additional organisations are to be added to this agreement.

12. Indemnity

Where a partner discloses inaccurate information which subsequently incurs liability, cost or expense, the disclosing organisation should indemnify the requesting organisation against such liability, cost or expense incurred.

This indemnity, however, should not apply in cases where the requesting organisation has been 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 organisation.

13. Monitoring and review

Both partners to this DSA will monitor any breaches or problems in relation to this agreement within their own organisations.

A review of the DSA will take place as per the review date on the opening page of this DSA 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 DSA 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 partner organisation listed as signatories.

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

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

8.2.2 All PID/PII 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 once it has fulfilled its purpose and is no longer needed.

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

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

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 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

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

The risks referred to in subsection (1) 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 you to take responsibility for complying with the principles, and to have appropriate processes and records in place to demonstrate that you comply.

The GDPR and the DPA relates specifically to PID/PII and how that information should be 'processed' (i.e. its collection, holding, use and information sharing). It applies to both

electronic and 'paper' forms. Both Acts provide enforceable principles of good practice. Anyone processing PID/PII (a Data Controller who should be registered) must ensure it meets the seven principles of the GDPR/DPA. This legislation gives significant rights to individuals in respect of personal data held about them by data controllers.

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 addition 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-ridden 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 PID/PII and means that individuals should be asked for permission to use their PID/PII 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. PID/PII 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 2001 (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

Appendix A. Signatory Sheet - Data Sharing Agreement

Organisation	Name	Position	Signature	Date
Nottinghamshire Healthcare NHS Foundation Trust	Julie Hankin	Executive Director of Nursing and Caldicott Guardian		
Nottinghamshire Healthcare NHS Foundation Trust	Andrew Haw	Data Protection Officer		
Nottinghamshire Social Care				
Age UK Connect	Michelle Elliott	Finance Director and Caldicott Guardian	MElliott	6/9/19
Ashfield District Council				
Mansfield District Council				

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 partners to this DSA are subject to a variety of legal, statutory and other 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: