University Hospitals of North Midlands NHS Trust

Information Sharing Agreement

Effective from Day Month 2019

Contents

1. Introduction

1.1. This Information Sharing Agreement has been agreed between

Organisation 1

University Hospitals of North Midlands NHS Trust

And

Organisation 2

1.2 This Agreement details the specific purpose(s), including legislative powers and duties, for sharing appropriate information, the operational procedures required (how & when this will happen), what data is to be shared, the consent processes involved and the process for review.

1.3 This Agreement is binding on both parties and each organisation will work towards meeting the commitments made. It is a working document and therefore the contents can be reviewed and altered at any time to reflect the changing circumstances. Such changes would be subject to the agreement of both parties.

1.4 The contents of this document must be summarised and distributed to appropriate operational/delivery staff within those organisations named above. The exact mechanism as to how this will be achieved will vary dependent upon internal communication structures.

1.5 A copy of this agreement, signed by all involved organisations, must be held by the UHNM. Copies of the document can be made available upon request.

2. Basis for Sharing

2.1 This agreement is between the partners listed in 1.1.

2.2 In order to share information between partners there must be a defined and justifiable purpose(s) which includes reference to any appropriate underpinning legislation (see Appendix 2).

2.3 The legal basis that underpins this relationship and the duties and powers to facilitate the lawful sharing of appropriate information between the named organisations are summarised as follows:

- GDPR Article 6(1)(e) - Necessary for the performance of a task carried out in the public interest/in the exercise of official authority vested in the controller

- GDPR Article 9(2)(h) special category data - processing is necessary for the purposes of the provision of health or social care or support or treatment or the management of health or social care systems and services on the basis of UK law.;
- Data Protection Act (2018)
- The Data Protection (Processing of Sensitive Personal Data) Order 2000/417
- The Human Rights Act 1998 (article 8);
- The Freedom of Information Act 2000
- Care Act 2014
- Health and Social Care Act 2008 (regulation of regulated activities), (Section 20)
- Common Law Duty of Confidentiality
- Caldicott 2 Principles
- Safeguarding Vulnerable Groups Act 2006
- Computer Misuse Act 1990;
- Mental Health Act 1983 and subsequent amendments 1995, 2001 and 2007
- Mental Capacity Act 2005

2.4 Any information shared and the processes used to share such information will be compliant with the relevant Human Rights legislation.

2.5 Both parties are responsible for ensuring their organisation complies with the National Data Guardian's 10 Data Security Standards

1. All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is shared for only lawful appropriate purposes.
2. All staff understand their responsibilities under the National Data Guardian's data security standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.
3. All staff complete appropriate annual data security training and pass a mandatory test, provided through the redesigned Information Governance Toolkit.
4. Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All instances of access to personal confidential data on IT systems can be attributed to individuals.
5. Processes are reviewed at least annually to identify and improve any which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.
6. Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken as soon as possible following a data

breach or near miss, with a report made to senior management within 12 hours of detection. Significant cyber-attacks are to be reported to CareCERT immediately following detection.

7. A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses and it is tested once a year as a minimum, with a report to senior management.
8. No unsupported operating systems, software or internet browsers are used within the IT estate.
9. A strategy is in place for protecting IT systems from cyber threats, based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.
10. IT suppliers are held accountable via contracts for protecting the personal confidential data they process and for meeting the National Data Guardian's data security standards.

3. Service Overview and Purpose

Name of Project, Initiative or Service	Click here to enter text.
Description (including outline of process)	Click here to enter text.
Purpose of the information sharing	Click here to enter text.
Benefits of information sharing	Click here to enter text.
Who is the information about? UHNM staff, UHNM patients, other? If "other" please provide details	Choose an item. If other please provide details.
Approximately how many people will have their information shared E.g., all Trust staff/all Trust patients/all patients in department/all patient with certain condition, etc. (please provide an estimate of numbers)	Click here to enter text.
Is information being sent to UHNM, sent from UHNM, (or both) or is the information accessed directly on site or remotely	Choose an item.
If an existing system will be utilised, provide the name of UHNM system information will be shared from or to	Click here to enter text.
Will information be sent abroad directly by UHNM or by the 3rd party? If yes, please provide details of the country and reason	Choose an item. If yes, please provide details.

4. Information Sharing Process and procedures

4.1 Information to be shared

4.1.1 Information shared between UHNM and Organisation 2 will be that which is necessary to safeguard, protect and promote the welfare of the Individual.

4.1.2 Under the General Data Protection Regulations (GDPR), the data protection principles set out the main responsibilities for organisations. Article 5 of the GDPR requires that personal data shall be:

a) Processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

4.1.3 If there is a need to share additional information on a one-off-basis, the parties concerned should consider whether the sharing is necessary to the agreement

and document their considerations/findings, including any consent sought (and if not sought, an explanation as to why).

4.1.4 If additional information is required on a repeated basis over and above what is defined in this agreement, to enable the agreement to achieve its aims, the lead officers for each organisation should agree an addition to the sharing agreement, ensuring that the new information meets the same legislative basis as the original. This addition should be added to the agreement and all parties should sign up to it.

4.1.5 The Data Sharing Table **in Section 6** contains summary details of what information can be shared, relevant contact details, methods of requesting and transferring information and the frequency of transfer for each item.

4.2 Ensuring Data Quality

4.2.1 All agencies are responsible for ensuring that they have processes and procedures in place for ensuring that information is recorded accurately, that there are methods in place for checking this and to ensure that shared information is of sufficient quality.

4.3 Information Use, Review, Retention and Deletion

4.3.1 Partners to this agreement undertake that information shared under the agreement will only be used for the specific purpose for which it was shared, in line with this agreement. It must not be shared for any other purpose outside of this agreement or be release to any third party without obtaining the express written authority of the partner who provided the information.

4.3.2 In line with each organisation's own retention policy, the information should not be kept any longer than is necessary.

4.3.3 The following destruction process will be used when the information is no longer required:

- Shredding (cross cut)
- Secure deletion from electronic devices; it is important that the data must be rendered unreadable when the device on which it resides is disposed of or recycled

Personal data which is ready for disposal should always be treated as confidential waste and must be kept secure at all times.

4.4 Subject Access Requests

4.4.1 If a request is received from a data subject to access records this will be dealt with by the relevant organisation in accordance with their respective procedures.

4.4.2 If shared data is involved, then the originating organisation should be informed of any disclosure and may advise on its release. However, the final decision will remain with the organisation who received the request.

5. Roles and Responsibilities

5.1 Roles and Responsibilities under this Agreement

5.1.1 All partners to this agreement are advised to appoint Specific Points of Contact (SPOC)

5.1.2 The people who will have access to information provided under this Agreement are:

UHNM (Organisation 1)	(Organisation 2)
Please list job roles of relevant staff, i.e. Treating Clinicians , Departmental receptionist etc.	

5.1.3 It is the responsibility of everyone sharing information and accessing and using the information that has been shared to take appropriate decisions and hold the information securely to UHNM standards. See addendum

5.1.4 The SPOC's within each organisation will be the first port of call for questions about the agreement. If there is a problem such as a potential data breach, relevant SPOCs must be contacted (and in the case of a potential data breach the Data Protection Officer of UHNM)

5.1.5 Only appropriate and properly authorised persons will have access to the information specified in this Agreement. If in doubt, a person intending to share or access information should contact their SPOC

5.2 Governance, Monitoring and Review

5.2.1 The review, monitoring and amendment of the agreement will be undertaken by the SPOC with advice from UHNM's Information Governance Department. Formal review will be undertaken annually unless legislation or policy changes dictate otherwise

5.2.2 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 to replace the old.

5.2.3 If the lead person departs their role, an alternative lead must be nominated as soon as possible

5.3 Indemnity

5.3.1 As receivers of information covered under this Agreement all signatories will accept total liability for a breach of this Information Sharing Agreement by their organisation should legal proceedings be served in relation to the breach.

5.4 Signatures

5.4.1 By signing this agreement, all signatories accept responsibility for its execution and agree to ensure that staff are trained so that requests for information and the process of sharing itself are sufficient to meet the purpose of this agreement.

5.4.2 Signatories must also ensure that they comply with all relevant legislation and with the provisions set out in this Agreement

6. Data Sets & Data Flow Mapping

What information will be shared? Please select **all** relevant fields.	☐ No Personal Information ☐ Name ☐ Address ☐ Postcode ☐ Date of Birth ☐ GP ☐ Consultant Name ☐ Next of Kin ☐ NHS Number ☐ Unit Number ☐ Treatment Types and Dates	☐ Gender ☐ Diagnosis ☐ Racial/Ethnic Origin ☐ Religion ☐ Occupation ☐ Political Opinion ☐ Medical History ☐ Sexual Orientation/Sex Life Information ☐ Genetic or Biometric data (i.e. gene sequence, fingerprints, facial recognition, retinal scanning) ☐ Other: Please State
Will any information be processed about …	Choose an item. Under 18's	Choose an item. Under 16's
Please select one of the following options that describes the personal information being sent;		
Identifiable ☐	The information shared is in an identifiable format (This doesn't have to include a person's name - it's anything that can identify them as an individual including their postcode, unit number, NHS number, etc.)	
Pseudonymised ☐	The identifiable information has been replaced with data	
Anonymised ☐	The data is fully anonymised and cannot be traced back to the patient	

Data Flow Map

Data Flow Description	From	To	Data Type	Bulk Data 50+	Transfer/Access method	Frequency	Where will the data be stored after access/transfer?	Purpose
			Personal, Special Category, anonymous, Pseudo	**Over 50 data subjects**	Electronic, secure email, hard copy, fax, post, courier etc. e.g. daily, weekly, monthly, on a certain date Reason for sharing including any legal obligation i.e. Care Act 2014	e.g. daily, weekly, monthly, on a certain date	**Secure onsite server/ locked filing cabinet**	Reason for sharing including any legal obligation i.e. Care Act 2014
Example: Patient referral	***UHNM***	***Organisation 2***	***Special category – Health***	***No***	***Electronic – Secure email Hard Copy – Post Courier***	***Weekly***	***Locked filing cabinet in locked office accessed by 3 people***	***Care Act 2014 Health and Social Care Act 2008 (regulation of regulated activities), (Section 20)***

7 List of Designated SPOCS & Data Breach reporting

Name of organisation	Spoc & Position Held	Contact Details (include Address, telephone Number & Email Address)
If the third party experience a breach which includes UHNM data they must contact UHNM straight away via infogovuhnm@uhnm.nhs.uk **Identifiable information should not be included in the email - please await further contact once the initial email has been sent.**		
If UHNM experience a breach of data and need to contact the 3rd party, please provide details of who they should contact	Click here to enter text.	

8. Information Sharing Agreement Authorisation

In signing this agreement you are agreeing to the UHNM sharing conditions in the introduction of this agreement.

Sharing is not authorised until this is signed on behalf of the Trust, agreements can only be signed by UHNM SIRO or Caldicott Guardian.

Third Party Acceptance & Participation			
Organisation Name			
DPA/ICO Registration No		Renewal Date Due	
Name			
Position			
Signature			
Date			
UHNM Acceptance & Participation			
DPA/ICO Registration No		Renewal Date Due	
Name			
Role			
Signature			
Date			

Appendix 1: Special Categories (formerly sensitive data)

Special category data means

Personal data consisting of information as to –

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- data concerning health or sex life and sexual orientation;
- genetic data (new); and
- biometric data where processed to uniquely identify a person (new)

Appendix 2: Conditions for processing

Lawfulness of processing conditions:

6(1) (a) - Verifiable consent of the data subject

6(1) (b) - Necessary for the performance of a contract with the data subject or to take steps to enter into a contract

6(1) (c) - Necessary for compliance with a legal obligation

6(1) (d) – Processing is necessary to protect the vital interests of a data subject or another Person

6(1)(e) - Necessary for the performance of a task carried out in the public interest/in the exercise of official authority vested in the controller

If special category data is also share you need to include one of these:

9(2)(a) - Verifiable explicit consent of the data subject

9(2)(b) - Necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement

9(2)(c) – Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent

9(2)(g) - Necessary for reasons of substantial public interest on the basis of EU/UK law which is proportionate to the aim pursued and which contains appropriate safeguards

9(2)(h) - Necessary for the purposes of:

- preventative or occupational medicine
- assessing the working capacity of the employee
- medical diagnosis
- the provision of health/social care or treatment or management of health/social care systems and
- services on the basis of EU/UK law
- a contract with a health professional
-

9(2)(I) - Necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products/medical devices

Information Sharing Agreement

Security Addendum

Information Governance

1.1 All organisations shall have in place appropriate internal information governance and/or operational policies and procedures to facilitate the effective processing of personal information which is relevant to the needs of the organisation, their managers/practitioners and their service users.

Staff Requirements

1.2 The conditions, obligations and requirements set out in the Information Sharing Arrangement and this Addendum apply to all appropriate staff, agency workers, and volunteers working within those organisations.

1.3 All organisations are strongly advised to ensure that staff have entered into appropriate confidentiality arrangements that detail the possible consequences of unauthorised or inappropriate disclosure of service user information. This may be incorporated into staff contracts if deemed necessary.

1.4 Each organisation must ensure that all appropriate staff have the necessary level of DBS clearance in accordance with relevant legislation and Government guidance.

Service User Awareness & Rights

1.5 Each organisation has a duty to ensure that all service users are aware of the information that is being collected and recorded about them, the reasons for doing so (including any statistical/analytical purposes), with whom it may be shared and why. This can be achieved by the issuing of a Privacy Notice (Fair Processing Notice).

1.6 Each organisation has a duty to ensure that all service users are aware of their rights in respect of information processing/sharing, including any limits and/or restrictions, in respect of Data Protection legislation, the Human Rights Act 1998, the Common Law Duty of Confidentiality and, where appropriate, the Freedom of Information Act 2000 and how these may be exercised.

1.7 This will include providing appropriate support in order that service-users may best exercise those rights; e.g. providing service users with information in alternative formats or languages or assisting them with a Subject Access Request.

1.8 All service users have a right to expect that information disclosed by them or by other parties about them, to an organisation will be treated with the appropriate degree of respect and confidence. This is covered by a Common Law Duty of Confidentiality. However, this right is not absolute and may be overridden in certain circumstances.

1.9 In addition, all service users must be made aware under what circumstances their consent will be required, and the procedure by which it will be sought, in order to obtain and share their personal information

Data Access & Security

1.10 Each organisation must ensure that appropriate technical and organisational measures are in place that protect against unauthorised or unlawful processing of personal information and against accidental loss or destruction of, or damage to, personal information. Thus:

- Each organisation must have in place a level of security commensurate with the sensitivity and classification of the information to be stored and/or shared, including information transferred to/received from other organisations.
- Each organisation must ensure that mechanisms are in place to address the issues of: physical security, security awareness and training, security management, systems development, role based security/practitioner access levels, data transfer and receiving and system specific security policies.
- Wherever 'Common Protective Markings' are used (OFFICIAL-SENSITIVE etc.) then each party organisation should agree and evidence the common meaning of these terms and the associated procedures in order to ensure that that the transmission/receipt and storage of information thus marked is appropriate to the level of security required.

Staff Awareness & Training

1.11 Each organisation has a responsibility to ensure that all relevant staff receive training, advice and on-going support in order to be made aware, and understand the implications, of:

- This Information Sharing Agreement (ISA) and any other associated documents (e.g. confidentiality agreement, the ISA, the 'Operational Arrangement', etc.). This is to include any associated operational requirements arising from the implementation of these.
- The underpinning and organisation specific legislation and associated regulations/guidance in respect of information sharing and any express or implied powers arising therefrom.
- Common Law duties (e.g. Confidentiality).
- Appropriate Codes of Practice and other associated regulations/guidance (e.g. NHS Confidentiality Code of Practice).

Designated Person

1.12 Each organisation must nominate a 'Designated Person' (e.g. Caldicott Guardian, Data Protection Officer, Knowledge Officer, other relevant manager, etc. - to be detailed on the ISA) with responsibility for ensuring that their organisation complies with legal and other appropriate requirements, obligations and guidance in respect of information processing and sharing, including those outlined in this and other related documents and arrangements.