Humber Information Sharing Charter

Version 10	Adopted: November 2020	Review Date: November 2022

This Charter may be an uncontrolled copy, before using please check the following website for the current version: https://www.nelincs.gov.uk/council-information-partnerships/information-governance/information-sharing/

This version supersedes all previous versions of this Charter including the Community Charter for Information Sharing (North East and North Lincolnshire) and the General Protocol for Information Sharing (Hull and the East Riding of Yorkshire).

1. Introduction and Purpose

1.1 Across the Humber we recognise that the sharing and processing of information is essential for delivering services and improving outcomes for the communities and individuals we serve. We take our data protection responsibilities seriously and recognise that there is a balance between the need to use and share information and maintaining the rights and privacy of individuals.

1.2 This Charter sets out our commitment to protecting personal data and ensuring good practice in our processing when working with partners, suppliers and processors.

1.3 The level of protection for data will be proportionate to the expectations of the data subjects, the sensitivity of the data and the likely consequences of its loss or misuse.

1.4 The Charter includes an Information Sharing Agreement template which can be used to document the purpose, lawful basis and operational arrangements for the use of personal data by partners, across traditional organisational boundaries, to achieve outcomes and deliver services.

1.5 This Charter is for guidance only and does not constitute a contract between those adopting it.

2. Scope

2.1 This charter applies where personal data is exchanged with partners exercising joint control over the data, as well as data processing arrangements in which one party processes data on behalf of or under the instructions of the other.

2.2 Personal data means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal data does not have to be confidential or private and could relate to anyone, including service users, employees etc.

3 Data Protection commitments and expectations

3.1 Through this Charter we commit to work to the data protection principles in the Data Protection Act 2018, data protection and information governance legislation, Codes of Practice and good practice, unless more stringent local law applies. These principles represent the minimum standard we will work, and we expect our delivery partners, suppliers and service providers to work to the same minimum standards. This means that in any data sharing or data processing arrangement, personal data will:

a) Be collected and used in ways that are lawful, fair and transparent – individuals will be told about what we do with their data and who we will disclose it to; it will only be used in ways they might reasonably expect; and nothing will be done with the data that would have an unjustifiably adverse effect on them.
b) Be collected and used only for specified and legitimate purposes – nothing will be done with the data that is incompatible with the purposes it is held for, unless required by law.
c) Be adequate, relevant and limited to what is necessary for the purpose – an approach of data minimisation will be followed with data only collected and used that is necessary to meet the

specified purpose. Wherever possible statistical, aggregated or anonymised information will be used to reduce the risk of individuals being identified.

d) Be maintained to appropriate quality standards – arrangements will be in place to ensure the accuracy of data including for correcting inaccurate data and keeping it up to date if necessary.
e) Be kept for no longer than is necessary – data will be managed in accordance with agreed retention standards, with arrangements in place for the de-identification of data / secure and confidential disposal.
f) Be protected from unauthorised use and disclosure or against accidental loss, destruction and damage – appropriate technical and organisational measures will be in place to keep data protected and secure and these will be regularly tested, assessed and evaluated for continued effectiveness. Examples include, access controls; audit trails; business continuity plans; network controls; robust policies and procedures; designated information governance roles and responsibilities Senior Information Risk Owner, Data Protection Officer, Caldicott Guardian; training and awareness raising activities for employees and those acting on behalf of the organisation; the pseudonymisation and encryption of personal data.
g) Be handled in line with the individual's rights – arrangements will be in place to ensure the rights of individuals are respected and can be exercised. The capacity of a individuals, including children and vulnerable adults, to exercise their rights will be considered case by case basis. Considerations of confidentiality and privacy will not automatically cease on death.
h) Not be transferred to other countries unless there is adequate protection for the rights of individuals in relation to their personal data – assurance of that adequate protection exists must be received before making such transfers. Shared personal data will not be transferred to other countries without first notifying the original data controller unless the transfer has already been agreed or is clearly implied by the circumstances.

3.2 Data controllers and processors are required to be able to demonstrate compliance with the principles. Partners will therefore ensure documented evidence is maintained of the steps taken to comply with the requirements of the Data Protection Act and other data protection legislation; and co-operate with each other were require.

3.3 When engaging data processors, only processors providing sufficient guarantees to implement appropriate technical and organisational measures to meet data protection legislation requirements and ensure the rights of the data subject will be used; and a written contract must be in place.

3.4 Data breaches, complaints, exercising of data subject rights including subject access and information requests will be processed in accordance with the established procedures of the partner identifying the incident and promptly notified to other relevant partners when necessary and relevant.

a) If a breach is severe enough to require reporting to the ICO this must be done within 72 hours of the incident being identified.
b) Many partners will be subject to the provisions of the Freedom of Information Act and Environmental Information Regulations which gives a general right of access to the information they hold. Any requests for information in relation to the Charter or Information Sharing Agreements will be processed in accordance with legal and statutory obligations following the receiving partner's established procedures and were appropriate jointly with partners.

3.6 It is recognised that in certain circumstances the processing of personal data may be affected by the exemptions in the Data Protection Act 2018 which might affect the commitments and expectations set out above. For example, the prevention of crime or the collection of taxes and duties. Where this is the case consideration will be given as to whether additional safeguards need to be put in place.

4 Other useful resources

4.1 Information Commissioner's Office website https://ico.org.uk/

5 Contact details

5.1 For more information about the Charter please email transparency@nelincs.gov.uk

Information Sharing Agreement

<Insert agreement title>

Agreement number: *<insert reference number>* Version No: *<insert review date>*

Review date: *<insert review date>*

1. Introduction

a) This agreement documents the lawful, fair, transparent, secure, and confidential sharing of information by the partners in section 2 of this agreement in accordance with data protection legislation and all other relevant legislation and codes of practice.

b) For the purpose of this agreement 'data protection legislation' means the General Data Protection Regulation and the Data Protection Act 2018.

c) Where applicable the Caldicott Principles as well as the Data Protection Principles will be complied with.

2. Parties to this agreement

<insert organisation name>
<insert organisation name>

a) Full details of each partner should be entered in Annex A.

3. Agreement implementation

a) This agreement comes into force from *<insert relevant date>*

b) This agreement applies *<insert relevant details for the agreement>*

c) Termination of this agreement must be in writing giving at least *<insert the relevant notice time if applicable – for some agreements this line may need to be deleted>* notice to the other partners.

4. Data Protection Impact Assessment (DPIA)

a) A DPIA is required whenever processing of personal is likely to result in a high risk to the rights and freedoms of individuals.
b) For the processing covered by this agreement

☐ A DPIA has been completed and signed off by all partners

☐ A DPIA has been considered and determined not to be necessary by all partners

☐ A DPIA is not required as no personal data is being processed

5. Purpose for the sharing of information

a) This agreement is designed to facilitate the sharing of information between the partners listed in section 2 for the purpose of:

<insert a brief description of the purpose the information will be used for that will assist transparency and public understanding; it may be easier to bullet point where there are multiple related purposes>.

b) Any information shared under this agreement, personal or otherwise, must only be used for the purpose(s) specified at the time of disclosure(s) except as required under statute or regulation, or under the instructions of a court.

6. The information to be shared

a) The partners agree that only the minimum necessary information relevant to the specified purpose will be shared and where possible aggregated or anonymised non-personal data will be used.

b) As part of this agreement the following information will be shared. A more detailed description of the information being shared can be found in the individual Data Set Lists (Annex B) supporting this agreement.

c) The personal data to be shared is:

<insert brief description of the personal data sets or data being shared i.e. NHS number, name, address, date of birth, etc.>

d) The special category personal data to be shared is:

<insert brief description of the special category personal data sets or data being shared i.e. health data, race or ethnic origin, etc.>

e) The criminal convictions and offences data to be shared is:

<insert brief description of the convictions and offence data sets or data being shared>

f) The non-identifiable data to be shared is:

<insert brief description of the non-identifiable data sets or data being shared i.e. performance statistics, financial information, etc.>

g) Data provided in a de-identified form (i.e. aggregated or anonymised) must not be knowingly or recklessly re-identified without the express consent of the data controller responsible for the de-identification.

7. The lawful, fair and transparent basis for the sharing of information

a) The basis for the sharing of information under this agreement is as follows.

b) The lawful basis for the sharing of personal data is:

<insert appropriate Article 6 details here. If consent is to be the basis for disclosure, then your agreement should detail how consent is obtained and address issues surrounding the withholding or withdrawal of consent. Please note for public authorities consent will not be a viable basis for processing in almost all cases.>

c) The lawful basis for the sharing of special category personal data is:

<insert appropriate Article 9 details and if appropriate the condition in Schedule 1. If consent is to be the basis for disclosure, then your agreement should detail how consent is obtained and address issues surrounding the withholding or withdrawal of consent. Please note for public authorities consent will not be a viable basis for processing in almost all cases.>

d) The lawful basis for the sharing of criminal convictions and offences data is:

<insert appropriate legal and / or official authority under Article 10 or if appropriate the schedule 1 condition met>

e) The lawful basis for the sharing of non-identifiable data is:

<insert the appropriate basis for the sharing of the information.>

8. The sharing process

a) Partners will share information in the following circumstances (**WHEN**):

<What will be the trigger or reason for the sharing of the information>

b) Partners will ensure that the information shared is accurate and if necessary, up to date (**QUALITY**): The following standards for accuracy and quality have been agreed.

<Please describe the agreed standards for the data>

c) Any discrepancies with the data should be reported to all relevant Partners immediately on discovery.

d) The disclosing partner will ensure that information is shared securely (**HOW**):

<What methods and measures will be used for the secure sharing of information>

e) Partners must ensure that only those with a clear and lawful requirement will have access to the shared information and have appropriate measures in place to limit access to those authorised. Access to the shared information will to be restricted to (**WHO**):

<Who will have access to the shared information and how will this be controlled>

f) The receiving partner will ensure that information is kept protected and secure (**HOW**):

<What measures will be in place to ensure the received information is kept protected and secure>

9. The disposal arrangements

a) Information will be securely disposed of by the receiving partner when no longer required for the purpose(s) it was shared for or to meet any legal or audit obligation (**DISPOSAL**):

<What measures will be in place to ensure the received information is kept protected and secure>

b) The retention period for the shared information is:

<Insert the timescales for the receiving partner to review the shared information to determine if they need to continue to hold it >

10. Security incidents/ personal data breaches

a) Security incidents/ personal data breaches (whether suspected or confirmed) shall be handled and investigated in accordance with the procedures of originating Partner.

b) Details of any breaches should be shared if relevant with Partner's SPOC as soon as is practicable so that appropriate action can be taken by them if necessary.

c) Where required under data protection legislation the ICO must be notified within 72 hours, and data subjects without undue delay to allow him or her to take the necessary precautions.

d) Each partner organisation will keep each of the other partners fully indemnified against any and all costs, expenses and claims arising out of any breach of this agreement and in particular, but without limitation, the unauthorised or unlawful access, loss, theft, use, destruction or disclosure by the offending partner or its subcontractors, employees, agents or any other person within the control of the offending partner of any personal data obtained in connection with this agreement.

11. Rights

a) Data protection legislation gives individuals certain rights over their personal data. These include the right to be informed; access personal data held about them; withdraw consent; request that inaccurate data is rectified and incomplete data is completed; be forgotten (erasure of data); restrict of processing; data portability; and to object to decisions made on the basis of automated processing and/or profiling.

b) Partners are responsible for ensuring they have supporting policies and procedures in place to support the exercise of these individual rights.

c) If appropriate Partners will notify other partners of any requests received.

12. Freedom of Information

a) The parties to this agreement acknowledge the Freedom of Information Act 2000 (hereinafter referred to as “FOIA”) and in particular that some parties may be required to provide information relating to this Agreement or the activity it supports in order to comply with their obligations under the FOIA.

b) All parties when dealing with a FOIA request will have due regard to the interests of the other parties.

c) All parties will facilitate each other’s compliance, in connection with this Agreement, with their obligations under the FOIA and shall comply with any reasonable request from the other for that purpose within 10 working days of the request being made.

13. Review

a) This agreement will be reviewed annually by the identified SPOC for *<insert name of organisation or organisations>*.

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

c) If a significant change takes place which means that the agreement is no longer fit for purpose, then the agreement will be updated as needed and a new version circulated.

d) If the partners to this agreement change, the agreement must be reviewed by the identified SPOC(s).

14. Signatories

By signing this agreement all partners accept responsibility for complying with current data protection legislation in the sharing of information and the standards and conditions set out within.

Name:

Organisation:

Position:

Signature:

Date:

Details of additional signatories can be added if required, or parties can sign separate copies.

Annex A – Partners to the agreement

Organisation name	
Organisation address	
Specific Point of Contact	
Position / Job title	
Contact number	
Email address	
ICO registration number	
NHS Data Security & Protection Toolkit Assurance	☐ Standards Met ☐ Standards Not Met (Plan agreed) ☐ Baseline Published ☐ Not Published ☐ Not applicable – NHS patient data & systems not accessed as part of this agreement

Organisation name	
Organisation address	
Specific Point of Contact	
Position / Job title	
Contact number	
Email address	
ICO registration number	
NHS Data Security & Protection Toolkit Assurance	☐ Standards Met ☐ Standards Not Met (Plan agreed) ☐ Baseline Published ☐ Not Published ☐ Not applicable – NHS patient data & systems not accessed as part of this agreement

Annex B – Data set list

Agreement number: *<insert ISA number>*

Data List number: *<insert number>*

1. Partners sharing information

a) Disclosing Partner: *<insert disclosing partner's name>*

b) Receiving Partner: *<insert receiving partner's name>*

c) Does the receiving partner become the Data Controller on receipt of the information?

☐ Yes ☐ No

2. Description of the information being shared

<Please insert description. If the information being shared is a specific system module or a report, please provide a description of the relevant module or report. If the information is a set of data items, considering providing in a table listing the field name, it's description and the format of the data e.g. DD/MM/YYYY.>

3. Information quality

a) Will any additional checks be made to the data prior to sharing?

☐ Yes (please provide details) ☐ No

<Please provide details of additional quality checks here>

4. Secure transfer of information (to be completed by disclosing partner)

a) Method of recording the disclosure of or access to information under this agreement

<Insert the business procedures in place to record the sharing of information, such as audit trials or disclosure logs>

b) Arrangements in place for the secure transfer of information

<Detail all the controls and business procedures in place for the secure exchange of information; examples include system access controls, encrypted USBs, secure e-mails, personal or courier delivery>

5. Secure receipt of information (to be completed by party receiving the information)

a) Arrangements in place for the secure receipt and storage of information

<Detail all the controls and business procedures in place for the secure receipt and ongoing storage of the shared information; examples include system and physical environment access controls>

b) Access to the information will be restricted to

<Detail as a minimum the team name and job title of the officers authorised to access the information. Where appropriate individual officers should be named>