External Ref:	HIG 01
Review date	November 2016
Version No.	V07
Internal Ref:	NELC 16.60.01

Humber Information Sharing Charter

This Charter may be an uncontrolled copy, please check the source of this document before use.

The latest version of the Charter can be found on the Humber data observatory website along with a list of the Charter signatories

http://www.humberdataobservatory.org.uk/legal

This Charter 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 between agencies in Kingston upon Hull and the East Riding of Yorkshire.

Contents

Humber Information Sharing Charter

Appendices

Humber Information Sharing Charter

1. Introduction

1.1 The appropriate exchange of information is essential to deliver effective and efficient services for our citizens, to meet their needs and ensure their welfare and protection. However there is a balance between the need to share sufficient information to deliver effective services, and preserving the privacy of the individual.

1.2 To assist understanding and the application of effective information sharing it is helpful to have locally documented clarity about how legal constraints 'fit' with practice guidelines, identifying what can and cannot be shared with whom, how and for what purposes.

1.3 This Charter provides a two-tier framework for the effective and secure sharing of information in accordance with legal requirements, ethical boundaries and good practice across the Humber region. It will ensure transparency of information governance practices, assist the documenting of information sharing decisions and actions to ensure they are auditable, and raise awareness of the legal and ethical boundaries around information disclosure and the rules and methods for accessing data.

1.4 Tier 1 (The Charter) establishes the Principles and standards under which information sharing will take place.

1.5 Tier 2 (The Agreements) identifies the operational requirements in place for the sharing of information for a specific and lawful purpose.

1.6 Whilst there will only be one Tier 1 Charter, there will be many Information Sharing Agreements.

1.7 The Charter does not impose new obligations on signatory organisations, but reflects current regulations and legislation for the sharing of personal information, and builds on existing partnerships.

2. Objectives of the Charter

2.1 The signatories to this Charter recognise the importance of sharing information effectively and securely for the purposes of delivering and improving outcomes for the citizens and communities we serve across the Humber Region.

2.2 Through this Charter the signatories aim to achieve consistent and good practice for the sharing of personal information.

- Providing signatory organisations and those acting on their behalf with clear guidelines to follow for the secure and confidential sharing of personal information in accordance with legal requirements.

- Informing citizens why personal information about them may need to be shared between signatory organisations, and how that information will be shared and used.

3 Our commitment

3.1 As a signatory organisation we are committed to ensuring that the identifiable personal information we collect, hold and use will be processed in accordance with legislation, best practice and the expectations of citizens, to meet and ensure security and confidentiality requirements. This Charter sets out the principles and minimum standards that will underpin the processing and exchange of personal information.

4 Designated Officer

4.1 As a signatory organisation we must have in place a Designated Officer, responsible for approving and monitoring the processing of personal information in accordance with the Humber Information Sharing Charter.

4.2 For Health and Social Care organisations this will be the Caldicott Guardian or the Senior Information Risk Owner, for organisations signed up to Public Service Networks it will be the Senior Information Risk Officer. For all other organisations it will be a senior officer with responsibility for information governance nominated by the Chief Executive or equivalent.

5 The principles guiding the sharing of information

5.1 As a signatory organisation we will work to:

a) Support and promote the accurate, timely, secure and confidential sharing of both person identifiable and anonymous information in accordance with our legal, statutory and common law duties, and the requirements of this Charter and other additional guidance as notified to us;

b) Ensure a copy of the Charter and the identity of the Designated Officer are clearly and widely promoted across the organisation and available to all;

c) Have in place effective policies and procedures to meet our responsibilities for the secure and confidential sharing of information, aligned to statutory requirements and this Charter;

d) Ensure that all employees and those acting on our behalf are aware of, understand and comply with their responsibilities for information security and confidentiality through appropriate promotion, training, monitoring and enforcement;

e) Ensure all our data meets the high standards identified in the Audit Commission's "Improving information to support decision making: standards for better quality data", November 2007, and any locally agreed protocols.

5.2 When sharing information we will endeavour to ensure that:

f) Individuals are fully informed about the information held about them and how it will be used and shared;

g) Information will be shared with consent, except where statutory requirements or common law principles support the disclosure or withholding of information;

h) Information is only shared when and where it is necessary and justified for a lawful and specified purpose;

i) Only the minimum identifiable information that is required for the purpose is shared. The information shared should be relevant, proportionate and not excessive for specified purpose, and be defined by the appropriate Tier 2 Protocol.

j) Wherever possible statistical or aggregated and anonymous information is provided, to eliminate the risk of individuals being identified;

k) Only information actually needed for the purpose will be collected or shared;

l) Information is clearly identified as being fact, opinion, or a combination of the two;

m) Information is only used for the purposes for which it was collected or shared;

n) Information is kept and shared safely and securely, with appropriate safeguards in place to ensure only individuals with a legitimate right have access to it, preventing accidental or deliberate unauthorised access;

o) Information no longer needed for legal or administration requirements is disposed of in a safe and appropriate manner;

p) The capacity of a data subject, including children and vulnerable adults, to exercise their right to provide or refuse consent will be considered on an individual case by case basis; and

q) Considerations of confidentiality and privacy will not automatically cease on death.

6 Tier 2 - Information Sharing Agreements

6.1 The focus of each agreement is the particular **purpose** underlying the need to share, who is sharing the information, the specific information being shared, the legal basis for the sharing of the information and the processes in place to ensure that the information is securely exchanged and managed.

6.2 Each Protocol describes the common contexts and shared objectives between signatory organisations delivering services of a similar scope, defines the type of information to be shared, the purposes for which it can be shared, and the underpinning legislation and the associated duties and powers that enable legally justifiable exchanges of information for that purpose based on the principles and standards set out in the Charter.

6.3 Tier 2 Agreements will be signed on behalf of each partner by a senior manager, with responsibility for operational delivery.

7 Information Security

7.1 It is assumed that each signatory has achieved or will aim to work towards information security standards such as ISO 27001, or a similar level of compatible security.

7.2 Each signatory is encouraged to have an Information Security Policy in place setting out the minimum standards of security they require. Where a specific policy is not in place the following principles must be followed at all times to ensure personal data is appropriately protected to prevent unauthorised access, disclosure, deletion or alteration:

a) Unauthorised officers and other individuals are prevented from gaining access to personal data;
b) Visitors must be supervised at all times;
c) All electronic systems containing personal data must be password-protected, to prevent unauthorised access;
d) Passwords must be treated as private to the individual and NOT disclosed to others;
e) All electronic devices including PCs, laptops and smartphones must be 'locked' when unattended or not in use;
f) All personal data stored on mobile electronic devices such as laptops, USBs, smartphones etc, must be protected by encryption;
g) All resources (including mobile devices, printouts) containing personal data must be placed in secure locations when not in use, and only accessible to authorised officers;
h) Anti-virus checks are undertaken on software / removable media prior to use on networks / machine;
i) All documents exchanged are protectively marked according to their sensitivity using the Government Protective Marking Classification Scheme;
j) Caution is exercised in the use of e-mail, recipients are checked and personal data is only exchanged using secure e-mail;
k) Caution is exercised in the use of fax communications, the intended recipient of a fax containing personal data must be aware that it is being sent and has ensured security on delivery;
l) Where personal data is removed from a secure environment, appropriate security measures must be in place to keep it secure and protected;
m) Caution is exercised in the use and transport of personal data outside of its secure environment or in the public domain to prevent loss or unauthorised disclosure;
n) Information must be disposed of securely; and
o) Personal data must not be disclosed to anyone other than the data subject unless you have their consent, or it is a registered disclosure, required by law, or permitted by a Data Protection Act 1998 exemption.

8 Signatory organisations to this Charter

8.1 A list of the organisations that have signed up to this Charter, and have agreed to adopt the principles and standards set out in it and the supporting agreements is available on the Humber data observatory website (http://www.humberdataobservatory.org.uk/legal)

9 Complaints

9.1 A complaint from a data subject or their representative about information held under the terms of this Charter will be investigated first by the signatory organisation receiving the complaint.

9.2 Where a complaint identifies that any part of the Charter needs to be reviewed, this action must be taken by the Humber Information Governance Group.

10 Freedom of Information

10.1 The Freedom of Information Act and Environmental Information Regulations gives a general right of access to the information public authorities hold. Any requests for information in relation to the Charter must be passed to the signatory organisation's Freedom of Information Officer to deal with.

10.2 Requests for Tier 2 Agreements will need to consider if the disclosure of any elements would compromise the procedures in place for the security and protection of the personal information, and potentially be subject to an exemption to disclosure.

11 Monitoring and Review

11.1 As a signatory to the Charter we agree to support the Humber Information Governance Group with the monitoring and 2 yearly review of the Charter and associated Tier 2 Agreements.

12 Humber Information Governance Group

12.1 The Humber Information Governance Group is a virtual Group representing public sector organisations and their partners across the Humber region.

13 Partnership undertaking

13.1 As a signatory to the Charter we accept the principles laid down in this document will provide a secure local framework between the signatory organisations for the secure sharing of personal information in a manner compliant with statutory and professional responsibilities.

13.2 On behalf of the organisation I represent, I confirm that we will undertake to comply with all relevant legislation and requirements relating to confidentiality, safe information sharing and disclosure, appropriate storage and destruction of information.

a) Implement and adhere to the standards and principles set out in this Charter whenever exchanging personal information, both with a co-signatories and other organisations;
b) Ensure that all Protocols and Procedures established for the sharing and confidentiality of information are consistent with this Charter;
c) Co-operate, as far is compatible with existing statutory responsibilities, with other signatories to ensure effective information sharing and reduce duplication.

13.3 Signatory

Organisation:	
Name:	
Position:	
Signature:	
Date:	

Appendix A Tier 2 - Information Sharing Agreement template

Insert here the logo
of the
signatory organisations

Agreement number	*<insert reference number>*
Review date	*<insert review date>*
Version No.	*<insert version number>*

Sharing information between partner organisations is vital to the provision of co-ordinated and seamless services. In addition, the sharing of information can help to meet the requirements of statutory and local initiatives. This agreement sets out the details for the secure and confidential sharing of personal information in accordance with the principles defined in the Humber Information Sharing Charter.

1. Purpose of the agreement

This agreement creates a framework for the formal exchange of personal information and intelligence between the partners to the agreement 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 – may be easier to bullet point where there are multiple related purposes>*.

Examples include

- *For the detection and prevention of crime including Facilitating a co-ordinated approach that targets crime and disorder*
- *For the administration of Housing Benefit - To assess and validate entitlement*
- *To deliver <insert particular service or outcomes>*
- *Managing the cost effective and appropriate allocation of resources to meet the needs of the data subject*

The following activities can and should normally be undertaken using aggregated non-personal information

- *Managing and planning service delivery*
- *Performance Management*
- *Identifying best practice*

2. Partners to the agreement

Name	*<insert the name of partner 1>*
Contact details	*<insert the contact details for partner 1>*
Data Notification Number	*<insert the number for partner 1>*

Name	*<insert the name of partner 2>*
Contact details	*<insert the contact details for partner 2>*
Data Notification Number	*<insert the number for partner 2>*

3. Implementation, review and termination of the agreement

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

b) This agreement will be reviewed at least annually, the date of the next review is *<insert date>*

c) This agreement can be suspended by either party in the event of a serious security breach. The suspension will be subject to a Risk Assessment and Resolution meeting between representatives of the partners, which should take place within 10 working days of any suspension.

d) Termination of this agreement must be in writing giving at least 30 days notice to the other partners.

e) If a new partner joins the agreement, a new version of the information sharing agreement will be issued as soon as possible, certainly within one month, and circulated to all participating parties.

f) If a partner leaves the agreement, a new version of the information sharing agreement will be issued as soon as possible, certainly within one month, to all participating parties. Partners must refer to section 6.9 regarding retention and deletion of information that has been shared.

g) 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.

4. Basis for the sharing of personal information

The sharing of personal information in accordance with this agreement is lawful under the Data Protection Act 1998 schedule 2 condition *<insert relevant condition>*

<Where sharing is based on consent please detail how consent is obtained and how consent can be withdrawn>

The sharing of sensitive personal information in accordance with this agreement is lawful under the Data Protection Act 1998 schedule 3 condition *<insert relevant condition>*

<Where sharing is based on consent please detail how consent is obtained and how consent can be withdrawn>

The primary legislation supporting the sharing of this information is: insert / delete as appropriate

<insert relevant legislation>

5. The personal information to be shared insert / delete as appropriate

5.1 *<insert the name of partner 1>* will share the following personal information

<insert brief description of relevant data sets or data field i.e. NHS number, name, address, date of birth, sex,>

5.2 *<insert the name of partner 2>* will share the following personal information

<insert brief description of relevant data sets or data field i.e. NHS number, name, address, date of birth, sex>

6. Processing of personal information

6.1 Personal information will be shared and processed by the partners in accordance with the Data Protection Act.

6.2 All information shared under this agreement, personal or otherwise, must only be used for the purpose(s) specified at the time of disclosure(s) as defined in the relevant data set list unless obliged under statute or regulation, or under the instructions of a court.

6.3 Where a partner receiving information under this agreement, wants to use that information for any other purpose, they must seek and receive permission from the original Data Controller before using the information for that further purpose. Further use of the information undertaken without the permission of the Data Controller will not be lawful or covered by this agreement.

6.4 The Data Protection Notification and Privacy Notice of each partner must reflect the processing of personal information under this agreement, to ensure that data subjects are fully informed about the information that is recorded about them and their rights to gain access to information held about them and to correct any factual errors that may have been made. If there are statutory grounds for restricting a data subject's access to the information held about them, they will be told that such information is held and the grounds on which it is restricted. Where opinion about a data subject is recorded and they feel the opinion is based on incorrect factual information, they will be given the opportunity to correct the factual error and / or record their disagreement with the recorded opinion.

6.5 Subject Access Requests will be handled in accordance with the standard procedures of the partner who receives the request.

6.6 Complaints will be handled in accordance with the standard procedures of the partner who receives the complaint.

6.7 The personal information shared under this agreement must be relevant and proportionate to achieve the purposes identified in section 1. Only the minimum necessary personal information will be shared and where possible aggregated non-personal information will be used.

6.8 The information shared should be complete (but not excessive), accurate and up-to-date to ensure all partners are assured that the information can be used for the purposes for which they require it.

6.9 The Data Controller must make all partners they share information with aware of their rules on data retention and whether these apply to the data being shared at the time of disclosure through the data set list (appendix B). The information must be securely disposed of when no longer required for the purpose(s) it was shared for or to meet any legal or audit obligation

7. Roles and responsibilities under the agreement

7.1 Each partner must appoint a single point of contact who must work together to jointly manage the valid and legally justified sharing of personal information for the purposes of this agreement; ensure the accuracy of the information shared; deal with data discrepancies; and ensure breaches are reported and investigated.

8. Signatories

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

Signatories must all ensure that they comply with all relevant legislation in the processing of personal information.

Signed on behalf of *<insert the details of partner 1>*

Name:	
Position:	
Signature:	
Date:	

Signed on behalf of *<insert the details of partner 2>*

Name:	
Position:	
Signature:	
Date:	

Signatory must be a senior manager of the organisation

Appendix B – Data set list

Data List number

Agreement number

Information disclosed by *<insert the name of partner disclosing data>* (Data Controller) to *<insert the name of partner receiving data>* for the specific purpose of *<insert the specific purpose here>*

No.	Data item	Data description (see note 1)	Format of data (see note 2)	Who is the Data Controller	How long will information be retained for
01					
02					
03					
04					
05					
06					
07					
08					
09					
10					

<insert additional lines if required>

All parties to the agreement must ensure that there is a common understanding of the data to be provided / received.

Note 1: The Data description should provide a clear definition of the data item. For example: **Contact Name = the name of the client's carer (usually relative or family friend) who may be contacted by professional careers.**

Note 2: The Format of data should provide a clear description of the format for data item. For example: **Date of Birth = DD/MM/YYYY**

1. Points of Contact

1.1 The point of contact for *<insert the name of partner disclosing data>* (Data Controller) is *<insert the name of officer>, <insert the name of appropriate role here>* has operational responsibility for the data

1.2 The point of contact for *<insert the name of partner receiving data>* is *<insert the name of officer>, <insert the name of appropriate role here>* has operational responsibility for the data

2. Information quality

2.1 The quality assurance checks applied to the shared information by the Data Controller are:

<The Data Controller should provide details here of the quality assurance procedures in place and how these are evidenced>

2.2 Partners receiving shared information are responsible for applying relevant quality assurance before using the information.

2.3 If information is found to be inaccurate, it is the responsibility of the partner discovering the inaccuracy to notify the Data Controller. The Data Controller will ensure that the source data is corrected and will notify all recipients, who will be responsible for updating the information they hold.

3. Information security and confidentiality

3.1 Arrangements in place for the secure exchange of information:

<Detail all the methods and business procedures to be used for sharing information; examples include encrypted USBs, secure e-mails, system access, at meetings>

3.2 Frequency for the sharing of information is:

<insert the frequency at which information will be shared>

3.3 The sharing of information will commence on:

3.4 The sharing of information will end on:

3.5 Disclosure of the information will be recorded as follows:

<insert the business procedures in place to record the sharing of information>

3.6 Arrangements the partner receiving the information has in place for keeping the information secure, protected and confidential:

<insert the business procedures in place to ensure the security and confidentiality of the information – reference section 7 of the Protocol>

3.7 The partner receiving the information will ensure that their employees:

a) are able to access only the shared information necessary for their role; and
b) are appropriately trained so that they understand their responsibilities for confidentiality and security.

3.8 The following employees of the partner receiving the information will have access to it:

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

3.9 Monitoring of security will be undertaken in light of each signatories established procedures.

4. Breaches of confidentiality

4.1 Breaches of data protection legislation will be dealt with by each partners established information security procedures and formal disciplinary procedures.

4.2 Details of confidentiality and data incidents will be notified to the point of contact of the other partner identified in section 1 of the Data List by the other partner within *<insert timescales>*

5. Retention and Disposal

5.1 The retention period for the shared information is:

<This section should detail the timescales for the receiving partner to review the shared information to determine if they need to continue to hold it >

5.2 The disposal method for the shared information when no longer required is:

<This section should detail the arrangements the receiving partner must follow for the disposal of the shared information when it is no longer necessary for them to hold the information >

5.3 The outcome of the review or destruction must be notified by the receiving partner to the Data Controller.